aws

Guida per gli sviluppatori

Amazon Simple Email Service

Amazon Simple Email Service: Guida per gli sviluppatori

Table of Contents

Che cos'è Amazon SES?

Amazon Simple Email Service (SES) è una piattaforma e-mail che offre un metodo semplice e conveniente per inviare e ricevere e-mail usando domini e indirizzi e-mail personali.

Puoi ad esempio inviare e-mail di marketing come offerte speciali, e-mail transazionali come conferme di ordini e altri tipi di corrispondenza, ad esempio newsletter. Quando usi Amazon SES per ricevere e-mail puoi elaborare soluzioni software, ad esempio strumenti di risposta automatica, sistemi per l'annullamento delle sottoscrizioni e-mail e applicazioni che generano ticket per il servizio clienti per le e-mail in arrivo.

Per informazioni e discussioni su differenti argomenti relativi ad Amazon SES, consulta il Blog di messaggistica e targeting AWS.

Vantaggi

La creazione di una soluzione e-mail su vasta scala è spesso un'attività complessa e costosa per le aziende. È necessario occuparsi di aspetti legati all'infrastruttura, ad esempio la gestione del server e-mail, la configurazione di rete e la reputazione degli indirizzi IP. Inoltre, molte soluzioni di e-mail di terze parti richiedono contratti e negoziazione di prezzi, così come costi iniziali significativi. Amazon SES elimina queste difficoltà e permette di sfruttare anni di esperienza e la sofisticata infrastruttura di e-mail creata da Amazon.com a servizio della sua vasta clientela.

Servizi correlati

Amazon SES si integra perfettamente con altri AWS prodotti. Ad esempio, sono possibili le seguenti operazioni:

- Aggiungere funzionalità di invio di e-mail a qualsiasi applicazione.
- Puoi inviare e-mail da Amazon EC2 servendoti di un SDK AWS, utilizzando l'interfaccia SMTP di Amazon SES oppure mediante chiamate dirette all'API Amazon SES.
- Utilizzare AWS Elastic Beanstalk per creare un'applicazione abilitata alle e-mail, ad esempio un programma che usi Amazon SES per inviare una newsletter ai clienti.
- Configurare Amazon Simple Notification Service (Amazon SNS) per informare in caso di mancato recapito di e-mail, e-mail che hanno provocato un reclamo o e-mail recapitate correttamente al

server di e-mail del destinatario. Quando si utilizza Amazon SES per ricevere e-mail, i contenuti della e-mail possono essere pubblicati negli argomenti di Amazon SNS.

- Usa il AWS Management Console per configurare Easy DKIM, che è un modo per autenticare le tue e-mail. Anche se è possibile usare Easy DKIM con qualsiasi fornitore DNS, la configurazione risulta particolarmente semplice quando si gestisce il dominio con Route 53.
- Controllare l'accesso degli utenti all'e-mail tramite AWS Identity and Access Management (IAM).
- Archiviare le e-mail ricevute su Amazon Simple Storage Service (Amazon S3).
- Intervenire sulle e-mail ricevute attivando funzioni AWS Lambda.
- Usare AWS Key Management Service (AWS KMS) per crittografare facoltativamente l'e-mail ricevuta su Amazon S3 bucket.
- Usare AWS CloudTrail per registrare le chiamate API di Amazon SES effettuate usando la console o l'API di Amazon SES.
- Pubblica i tuoi eventi di invio e-mail su Amazon CloudWatch o Amazon Data Firehose. Se pubblichi i tuoi eventi di invio e-mail su Firehose, puoi accedervi in Amazon Redshift, AmazonService o OpenSearch Amazon S3.

Prezzi

Con Amazon SES, paghi in base al volume delle email inviate e ricevute. Per ulteriori informazioni, consulta la pagina dei Prezzi di Amazon SES.

Regioni e Amazon SES

Amazon SES è disponibile in diverse AWS regioni del mondo. In ogni regione, AWS gestisce più zone di disponibilità. Queste zone di disponibilità sono fisicamente isolate l'una dall'altra, ma sono unite da connessioni di rete private a bassa latenza, a velocità effettiva elevata e altamente ridondanti. Queste zone di disponibilità ci consentono di fornire livelli molto elevati di disponibilità e ridondanza, riducendo al minimo la latenza.

Per un elenco di URL di endpoint SMTP per le in cui è disponibile Amazon SES, consulta Amazon Simple Email Service (Amazon SES) in Riferimenti generali di AWS. Per ulteriori informazioni sul numero di zone di disponibilità presenti in ciascuna Regione, consulta Infrastruttura globale di AWS.

Questa sezione contiene informazioni che devi sapere se prevedi di utilizzare Amazon SES in più AWS regioni. Sono illustrati i seguenti argomenti:

- Regioni ed endpoint Amazon SES
- Rimozione della sandbox e aumento dei limiti di invio
- Verifica di indirizzi e-mail e domini
- Easy DKIM
- Elenco di eliminazione a livello di account
- Notifiche di feedback
- Credenziali SMTP
- Autorizzazione di invio
- Domini MAIL FROM personalizzati
- Ricezione di e-mail
- Impostazione dei record (MX)

Per informazioni generali sulle AWS regioni, consulta gli endpoint di AWS servizio nella Guida AWS generale.

Regioni ed endpoint Amazon SES

Quando utilizzi Amazon SES per inviare e-mail, puoi connetterti a un URL che fornisce un endpoint per l'API SES o per l'interfaccia SMTP. Riferimenti generali di AWS contiene l'elenco completo degli endpoint che usi per inviare e ricevere email con Amazon SES. Per ulteriori informazioni, consulta Endpoint e quote di Amazon Simple Email Service in Riferimenti generali di AWS.

Quando invii email tramite Amazon SES, puoi usare gli URL nelle righe specificate con HTTPS nella colonna Protocollo per effettuare richieste HTTPS all'API SES. Puoi anche utilizzare gli URL nelle righe specificate con SMTP nella colonna Protocollo per inviare email tramite l'interfaccia SMTP.

Se hai configurato Amazon SES per ricevere le e-mail inviate al tuo dominio, puoi utilizzare gli URL dell'endpoint SMTP in entrata (ovvero gli URL che iniziano con "inbound-smtp") quando configuri i record di Mail Exchanger (MX) nelle impostazioni DNS per il tuo dominio.

> **Note**
>
> Gli URL SMTP in entrata non sono indirizzi del server IMAP. In altre parole, non possono essere utilizzati per ricevere e-mail utilizzando un'applicazione come Outlook. Per un servizio che fornisce un server IMAP per la posta elettronica in arrivo, consulta Amazon. WorkMail

Rimozione della sandbox e aumento dei limiti di invio

Lo stato della sandbox del tuo account può variare a seconda delle regioni. AWS In altre parole, se il tuo account è stato rimosso dalla sandbox nella Regione Stati Uniti occidentali (Oregon), è possibile che sia ancora presente nella sandbox della Regione Stati Uniti orientali (Virginia settentrionale) a meno che non sia stato rimosso.

I limiti di invio possono anche variare a seconda della AWS regione. Ad esempio, se il tuo account è in grado di inviare 10 messaggi al secondo nella Regione Europa (Irlanda), potresti essere in grado di inviare più o meno messaggi in altre Regioni.

Quando invii una richiesta per rimuovere il tuo account dalla sandbox oppure quando invii una richiesta per aumentare le quote di invio del tuo account, assicurati di scegliere tutte le regioni AWS a cui si applica la tua richiesta. È possibile inviare diverse richieste in una singola pratica del Centro assistenza.

Verifica di indirizzi e-mail e domini

Prima di poter inviare e-mail usando Amazon SES, è necessario accertarsi di essere i proprietari del dominio o dell'indirizzo e-mail da cui si intende inviare. Lo stato di verifica degli indirizzi e-mail e dei domini varia anche a seconda delle regioni AWS . Ad esempio, se verifichi un dominio nella Regione Stati Uniti occidentali (Oregon), non è possibile utilizzare quel dominio per inviare e-mail nella Regione Stati Uniti orientali (Virginia settentrionale) fino al completamento della procedura di verifica per quella Regione. Per ulteriori informazioni sulla verifica di indirizzi e-mail e domini, consulta Identità verificate in Amazon SES.

Easy DKIM

Il processo di configurazione di Easy DKIM deve essere eseguito per ogni regione in cui desideri utilizzare questa funzionalità. Pertanto, in ciascuna Regione, è necessario utilizzare la console o l'API Amazon SES per generare record TXT. Successivamente, devi aggiungere tutti i record TXT alla configurazione DNS per il tuo dominio. Per ulteriori informazioni sulla configurazione di Easy DKIM, consulta Easy DKIM in Amazon SES.

Elenco di eliminazione a livello di account

Il tuo elenco di soppressioni a livello di account Amazon SES si applica Account AWS solo al tuo account corrente. Regione AWS Puoi aggiungere o rimuovere manualmente, singolarmente o in

blocco, indirizzi dall'elenco di eliminazione a livello di account utilizzando l'API SES v2 o la console. Per ulteriori informazioni sull'utilizzo dell'elenco di eliminazione a livello di account, consulta Utilizzo dell'elenco di eliminazione a livello di account di Amazon SES.

Notifiche di feedback

Due importanti punti da considerare riguardano la configurazione di notifiche di feedback in più regioni:

- Le impostazioni delle identità verificate, come la ricezione di feedback tramite e-mail o Amazon Simple Notification Service (Amazon SNS), si applicano solo alla Regione in cui vengono impostate. Ad esempio, se verifichi user@example.com nelle regioni Stati Uniti occidentali (Oregon) e Stati Uniti orientali (Virginia settentrionale) e intendi ricevere le e-mail non recapitate tramite notifiche Amazon SNS, devi utilizzare l'API o la console Amazon SES per configurare le notifiche di feedback Amazon SNS per user@example.com in entrambe le regioni.
- Gli argomenti Amazon SNS utilizzati per l'inoltro di feedback devono trovarsi all'interno della stessa regione in cui utilizzi Amazon SES.

Credenziali SMTP

Le credenziali utilizzate per inviare e-mail tramite l'interfaccia SMTP di Amazon SES sono uniche per ogni AWS regione. Se utilizzi l'interfaccia SMTP Amazon SES per l'invio di e-mail in più di una Regione, è necessario generare un set di credenziali SMTP per ogni Regione.

> **Note**
>
> Se hai creato le credenziali SMTP prima del 10 gennaio 2019, le credenziali SMTP sono state create utilizzando una versione precedente della firma. AWS Per motivi di sicurezza, devi eliminare le credenziali create prima di questa data e sostituirle con credenziali più recenti. Puoi eliminare le credenziali più vecchie usando la console IAM.

Domini MAIL FROM personalizzati

Puoi utilizzare lo stesso dominio MAIL FROM personalizzato per le identità verificate in diverse regioni AWS . A questo scopo, devi solo pubblicare un record MX nel server DNS del dominio MAIL FROM. In questo caso, le notifiche di mancato recapito vengono inviate all'endpoint di feedback

Amazon SES nella Regione specificata nel record MX. Quindi, Amazon SES reindirizza i mancati recapiti all'identità verificata nella Regione che ha inviato l'e-mail.

Utilizza le impostazioni dei record MX fornite da Amazon SES durante il processo di configurazione del dominio MAIL FROM personalizzato per un'identità in una delle regioni. Il processo di configurazione del dominio MAIL FROM personalizzato è descritto in Uso di un dominio MAIL FROM personalizzato. Come riferimento, nella tabella seguente sono riportati gli endpoint di feedback di tutte le regioni.

Nome della Regione	Endpoint di feedback per le configurazioni di invio del dominio MAIL FROM personalizzato
Stati Uniti orientali (Ohio)	feedback-smtp.us-east-2.amazonses.com
Stati Uniti orientali (Virginia settentrionale)	feedback-smtp.us-east-1.amazonses.com
Stati Uniti occidentali (California settentrionale)	feedback-smtp.us-west-1.amazonses.com
US West (Oregon)	feedback-smtp.us-west-2.amazonses.com
Africa (Città del Capo)	feedback-smtp.af-south-1.amazonses.com
Asia Pacifico (Giacarta)	feedback-smtp.ap-southeast-3.amazonses.com
Asia Pacifico (Mumbai)	feedback-smtp.ap-south-1.amazonses.com
Asia Pacifico (Osaka-Locale)	feedback-smtp.ap-northeast-3.amazonses.com
Asia Pacifico (Seul)	feedback-smtp.ap-northeast-2.amazonses.com
Asia Pacifico (Singapore)	feedback-smtp.ap-southeast-1.amazonses.com
Asia Pacifico (Sydney)	feedback-smtp.ap-southeast-2.amazonses.com
Asia Pacifico (Tokyo)	feedback-smtp.ap-northeast-1.amazonses.com
Canada (Centrale)	feedback-smtp.ca-central-1.amazonses.com
Europa (Francoforte)	feedback-smtp.eu-central-1.amazonses.com
Europa (Irlanda)	feedback-smtp.eu-west-1.amazonses.com

Nome della Regione	Endpoint di feedback per le configurazioni di invio del dominio MAIL FROM personalizzato
Europa (Londra)	feedback-smtp.eu-west-2.amazonses.com
Europa (Milano)	feedback-smtp.eu-south-1.amazonses.com
Europa (Parigi)	feedback-smtp.eu-west-3.amazonses.com
Europa (Stoccolma)	feedback-smtp.eu-north-1.amazonses.com
Israele (Tel Aviv)	feedback-smtp.ca-central-1.amazonses.com
Medio Oriente (Bahrein)	feedback-smtp.me-south-1.amazonses.com
Sud America (San Paolo)	feedback-smtp.sa-east-1.amazonses.com
AWS GovCloud (Stati Uniti occidentali)	feedback-smtp. us-gov-west-1.amazonses.com
AWS GovCloud (Stati Uniti orientali)	feedback-smtp. us-gov-east-1.amazonses.com

Autorizzazione di invio

I mittenti delegati possono inviare e-mail solo dalla AWS regione in cui è verificata l'identità del proprietario dell'identità. La policy di autorizzazione di invio che concede l'autorizzazione al mittente delegato deve essere collegata all'identità in questa regione. Per ulteriori informazioni sull'autorizzazione all'invio, consulta Uso dell'autorizzazione di invio con Amazon SES.

Ricezione di e-mail

Ad eccezione dei bucket Amazon S3, tutte le AWS risorse utilizzate per ricevere e-mail con Amazon SES devono trovarsi nella stessa AWS regione dell'endpoint Amazon SES. Ad esempio, se utilizzi Amazon SES nella regione Stati Uniti occidentali (Oregon), allora ogni argomento Amazon SNS, chiave AWS KMS e funzione Lambda utilizzati devono trovarsi nella Regione Stati Uniti occidentali (Oregon). Analogamente, per ricevere e-mail con Amazon SES all'interno di una regione, è necessario creare una regola di ricezione attiva configurata in tale Regione.

La tabella seguente elenca gli endpoint di ricezione e-mail per tutte le AWS regioni in cui Amazon SES supporta la ricezione di e-mail:

Nome della regione	Regione	Endpoint di ricezione e-mail
US East (N. Virginia)	us-east-1	inbound-smtp.us-east-1.amazonaws.com
Stati Uniti orientali (Ohio)	us-east-2	inbound-smtp.us-east-2.amazonaws.com
US West (Oregon)	us-west-2	inbound-smtp.us-west-2.amazonaws.com
Asia Pacifico (Giacarta)	ap-southeast-3	inbound-smtp.ap-southeast-3.amazonaws.com
Asia Pacific (Singapore)	ap-southeast-1	inbound-smtp.ap-southeast-1.amazonaws.com
Asia Pacific (Sydney)	ap-southeast-2	inbound-smtp.ap-southeast-2.amazonaws.com
Asia Pacifico (Tokyo)	ap-northeast-1	inbound-smtp.ap-northeast-1.amazonaws.com
Canada (Central)	ca-central-1	inbound-smtp.ca-central-1.amazonaws.com
Europe (Frankfurt)	eu-central-1	inbound-smtp.eu-central-1.amazonaws.com
Europa (Irlanda)	eu-west-1	inbound-smtp.eu-west-1.amazonaws.com
Europe (London)	eu-west-2	inbound-smtp.eu-west-2.amazonaws.com

SES non supporta la ricezione di e-mail nelle seguenti regioni: Stati Uniti occidentali (California settentrionale), Africa (Città del Capo), Asia Pacifico (Mumbai), Asia Pacifico (Osaka), Asia Pacifico (Seoul), Europa (Milano), Europa (Parigi), Europa (Stoccolma), Israele (Tel Aviv), Medio Oriente

(Bahrain), Sud America (San Paolo), AWS GovCloud (Stati Uniti occidentali) e AWS GovCloud (Stati Uniti orientali).

Quote di servizio in Amazon SES

Le sezioni seguenti elencano e descrivono le quote applicabili alle risorse e alle operazioni Amazon SES. Alcune quote possono essere aumentate, al contrario di altre. Per determinare se puoi richiedere un aumento per una quota, consulta la colonna Adjustable (Regolabile).

> **Note**
>
> Le quote SES si riferiscono a ciascuna di quelle Regione AWS che utilizzi nel tuo. Account AWS

Quote di invio e-mail

Le seguenti quote si applicano all'invio di e-mail tramite SES.

Quote di invio

Le quote si basano sul numero di destinatari e non sul numero di messaggi.

Risorsa	Quota predefinita	Regolabile
Numero di e-mail che è possibile inviare in un periodo di tempo di 24 ore	Se il tuo account è nella sandbox, puoi inviare fino a 200 e-mail per ogni periodo di 24 ore. Se l'account è esterno alla sandbox, questo numero varia in base al caso d'uso specifico .	Sì
Numero di e-mail che è possibile inviare al secondo (frequenza di invio)	Se il tuo account è nella sandbox, puoi inviare 1 e-mail al secondo.	Sì

Risorsa	Quota predefinita	Regolabile
	Se l'account è esterno alla sandbox, questa frequenza varia in base al caso d'uso specifico.	

Quote dei messaggi

Risorsa	Quota predefinita	Regolabile
Utilizzo dell'API SES v1: dimensione massima del messaggio (compresi gli allegati)	10 MB per messaggio (dopo la codifica base64).	No Per carichi di lavoro con dimensioni di messaggi superiori a 10 MB, valutare la migrazione all'API SES v2.
Utilizzo dell'API SES v2 o SMTP: dimensione massima del messaggio (compresi gli allegati)	40 MB per messaggio (dopo la codifica base64).	No

> **Note**
>
> I messaggi di dimensioni superiori a 10 MB sono soggetti a limitazione della larghezza di banda e, a seconda della velocità di invio, si potrebbe verificare una limitazione a 40 MB/s. Ad esempio, è possibile inviare un messaggio di 40 MB alla velocità di 1 messaggio al secondo o due messaggi da 20 MB al secondo.

Quote per mittenti e destinatari

Risorsa	Quota predefinita	Regolabile
Numero massimo di destinatari per messaggio	50 destinatari per messaggio.	Questo limite destinatario non è regolabile. Contatta il tuo AWS Account Manager per

Risorsa	Quota predefinita	Regolabile
	Note Un destinatario è qualsiasi indirizzo indicato nei campi "A", "CC" o "CCN".	richiedere questa funzionalità dopo aver letto la nota seguente.
Numero massimo di identità che è possibile verificare	10.000 identità per. Regione AWS **Note** Un'identità è un dominio o un indirizzo e-mail utilizzato per inviare e-mail tramite SES.	Contatta il tuo AWS Account Manager per discutere il tuo caso d'uso.
Numero massimo di pool IP dedicati (inclusi pool IP gestiti e standard)	50	No

Note

Prima di richiedere un aumento del limite di destinatari per messaggio, leggi questo blog e prepara una descrizione dettagliata del motivo per cui il tuo caso d'uso non è in linea con il limite predefinito di 50 destinatari per messaggio, né con l'invio dei messaggi a singoli destinatari. La definizione di più destinatari in una destinazione del messaggio può comportare una scarsa osservabilità e uno scarso recapito e non deve essere utilizzata a meno che il caso d'uso non lo richieda specificamente.

Quote relative alla pubblicazione di eventi

Risorsa	Quota predefinita	Regolabile
Numero massimo di set di configurazione	10.000	No
Lunghezza massima del nome del set di configurazione	I nomi dei set di configurazione possono contenere fino a 64 caratteri alfanumerici. Possono inoltre contenere trattini (-) e caratteri di sottolineatura (_). I nomi non possono contenere spazi, caratteri accentati o altri caratteri speciali.	No
Numero massimo di destinazioni di eventi per ogni set di configurazione	10	No
Numero massimo di dimensioni per destinazione CloudWatch dell'evento	10	No

Quote dei modelli di e-mail

Risorsa	Quota predefinita	Regolabile
Numero massimo di modelli di e-mail in ciascuno Regione AWS	20.000	No
Dimensione massima del modello	500 KB	No

Risorsa	Quota predefinita	Regolabile
Numero massimo di valori di sostituzione in ogni modello	Illimitato	N/D
Numero massimo di destinatari per ogni modello di e-mail	50 destinazioni. Una destinazione consiste in qualsiasi indirizzo e-mail indicato nei campi "A", "CC" o "CCN". **Note** Il numero di destinazioni che puoi contattare in una sola chiamata all'API potrebbe essere limitato dalla frequenza massima in uscita del tuo account.	No

Quote di ricezione di e-mail

La tabella seguente elenca le quote associate alla ricezione di e-mail tramite SES.

Risorsa	Quota predefinita	Regolabile
Numero massimo di regole per set di regole di ricezione	200	No
Numero massimo di operazioni per regola di ricezione	10	No
Numero massimo di destinatari per regola di ricezione	100	No

Risorsa	Quota predefinita	Regolabile
Numero massimo di set di regole di ricezione per Account AWS	40	No
Numero massimo di filtri per indirizzi IP per Account AWS	100	No
Dimensione massima di e-mail (incluse intestazioni) che può essere archiviata in un bucket Amazon S3	40 MB	No
Dimensione massima di e-mail (incluse intestazioni) che può essere pubblicata utilizzando una notifica Amazon SNS	150 KB	No

Quote di Mail Manager

La tabella seguente elenca le quote associate a Mail Manager.

Risorsa	Quota predefinita	Regolabile
Numero massimo di endpoint di ingresso aperti	10	No
Numero massimo di endpoint di ingresso autorizzati	50	No
Numero massimo di destinatari per messaggio	100	No
Dimensione massima delle e-mail (incluse le intestazioni)	40 MB	No

Risorsa	Quota predefinita	Regolabile
Numero massimo di dichiarazioni sulla politica del traffico	20	No
Numero massimo di condizioni dichiarate sulla politica del traffico	10	No
Numero massimo di politiche di traffico per regione	100	No
Numero massimo di relè SMTP	100	No
Numero massimo di set di regole	40	No
Numero massimo di esecuzioni di regole per messaggio	200	No
Numero massimo di condizioni per regola	10	No
Numero massimo di azioni per regola	10	No
Numero massimo di azioni di inoltro o invio per set di regole	10	No
Numero massimo di archivi attivi	10	No
Numero massimo di richieste di ricerca in esecuzione in parallelo	1	No

Risorsa	Quota predefinita	Regolabile
Numero massimo di richieste di esportazione in esecuzione in parallelo	1	No
Numero massimo di modifiche di conservazione per l'archivio a settimana	1	No

Quote generali

La tabella seguente elenca le quote che si applicano sia all'invio che alla ricezione di e-mail tramite SES.

Quote di invio tramite API SES

Risorsa	Quota predefinita	Regolabile
Frequenza a cui puoi chiamare le operazioni API Amazon SES	Tutte le operazioni (fatta eccezione per `SendEmail`, `SendRawEmail` e `SendTemplatedEmail`) vengono limitate a una richiesta al secondo.	No
Parti MIME	500	No

Tipi di credenziali Amazon SES

Per interagire con Amazon Simple Email Service (Amazon SES), è necessario usare le credenziali di sicurezza per verificare la propria identità e se si dispone dell'autorizzazione per interagire con Amazon SES. Ci sono diversi tipi di credenziali e quelle utilizzate dipendono dalle operazioni da eseguire. Ad esempio, è possibile usare le chiavi di accesso AWS per inviare un'e-mail con l'API Amazon SES o le credenziali SMTP per inviare un'e-mail con l'interfaccia SMTP di Amazon SES.

La tabella seguente elenca i tipi di credenziali che è possibile usare con Amazon SES, a seconda delle operazioni da eseguire.

Se desideri accedere a...	Usa queste credenziali	Tipo di credenziali	Come ottenere le credenziali
API Amazon SES (Puoi accedere all'API Amazon SES direttamente o indirettamente attraverso un SDK AWS, AWS Command Line Interface o AWS Tools for Windows PowerShell.)	Chiavi di accesso AWS	ID chiave di accesso e chiave di accesso segreta	Consulta la pagina relativa alle chiavi di accesso in Riferimenti generali di AWS. **Note** Come best practice per la sicurezza , usa chiavi di accesso utente AWS Identity and Access Management (IAM) invece di chiavi di accesso Account AWS. Le credenzia li Account AWS concedono accesso completo a tutte le risorse AWS, quindi è necessario archiviar le in un luogo sicuro e usare invece le credenziali utente IAM per l'interazione quotidiana con AWS. Per ulteriori informazi oni, consulta la pagina relativa a credenzia li dell'account root e credenziali utente IAM

Se desideri accedere a...	Usa queste credenziali	Tipo di credenziali	Come ottenere le credenziali
			in Riferimenti generali di AWS.

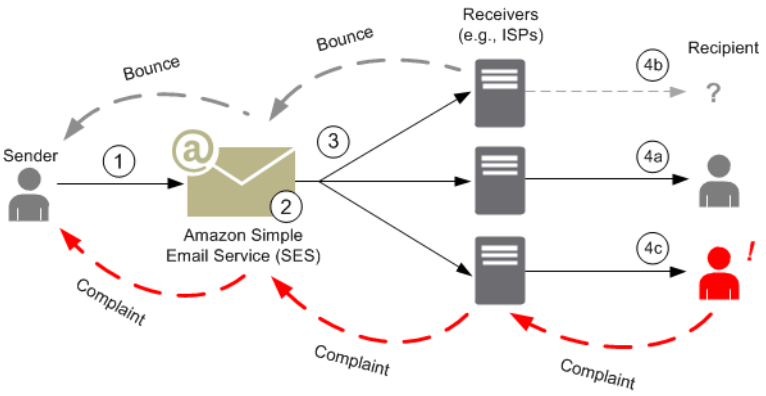
Se desideri accedere a...	Usa queste credenziali	Tipo di credenziali	Come ottenere le credenziali
Interfaccia SMTP di Amazon SES	Credenziali SMTP	Nome utente e password	Per informazioni, consultare [Richiesta delle credenziali SMTP Amazon SES](). **Note** Anche se le credenziali SMTP di Amazon SES sono diverse rispetto alle chiavi di accesso AWS e alle chiavi di accesso utente IAM, le credenziali SMTP di Amazon SES sono effettivamente un tipo di credenziali IAM. Un utente IAM può creare credenziali SMTP di Amazon SES, ma il proprietario dell'account root deve assicurare che le policy dell'utente IAM conferiscano l'autorizzazione di accesso alle operazioni IAM seguenti: "iam:ListUsers", "iam:CreateUser", "iam:CreateAccessKey" e "iam:PutUserPolicy".

Se desideri accedere a...	Usa queste credenziali	Tipo di credenziali	Come ottenere le credenziali
Console Amazon SES	Nome utente e password IAM O Indirizzo e-mail e password	Nome utente e password IAM O Indirizzo e-mail e password	Consulta le pagine relative a nome utente e password IAM e indirizzo e-mail e password in Riferimenti generali di AWS. **Note** Come best practice per la sicurezza, usa nome utente e password IAM invece di indirizzo e-mail e password. La combinazione di indirizzo e-mail e password serve per l'Account AWS, quindi è necessario archiviare queste credenziali in un luogo sicuro invece di usarle per l'interazione quotidiana con AWS. Per ulteriori informazioni, consulta la pagina relativa a credenziali dell'account root e credenziali utente IAM in Riferimenti generali di AWS.

Per ulteriori informazioni sui diversi tipi di credenziali di sicurezza AWS (ad eccezione delle credenziali SMTP, usate solo per Amazon SES), consulta la pagina relativa alle credenziali di sicurezza AWS in Riferimenti generali di AWS.

Come funziona l'invio di e-mail in Amazon SES

In questo argomento viene illustrato cosa succede quando si invia un'e-mail con SES e i diversi risultati che si possono ottenere dopo l'invio. La figura seguente rappresenta un riepilogo generale del processo di invio:



1. Un'applicazione client, che agisce come mittente dell'e-mail, effettua una richiesta a SES per l'invio di e-mail a uno o più destinatari.
2. Se la richiesta è valida, SES accetta l'e-mail.
3. SES invia il messaggio tramite Internet al ricevitore del destinatario. Una volta che il messaggio viene passato a SES, di solito viene inviato immediatamente, con il primo tentativo di consegna che normalmente si verifica entro pochi millisecondi.
4. A questo punto, si presentano diverse possibilità. Ad esempio:
    a. L'ISP consegna il messaggio nella casella di posta in arrivo del destinatario.
    b. L'indirizzo e-mail del destinatario non esiste, pertanto l'ISP invia una notifica di mancato recapito a SES. SES inoltra quindi la notifica al mittente.
    c. Il destinatario riceve il messaggio, ma lo considera spam e registra un reclamo con l'ISP. L'ISP, per il quale è configurato un loop di feedback con SES, invia il reclamo a SES che, quindi, lo inoltra al mittente.

Nelle seguenti sezioni vengono esaminati i singoli risultati possibili dopo l'invio a SES di una richiesta di e-mail da parte di un mittente e dopo l'invio di un messaggio e-mail al destinatario da parte di SES.

Dopo l'invio a SES di una richiesta di e-mail da parte di un mittente

Quando il mittente effettua una richiesta a SES per l'invio di un'e-mail, la chiamata può riuscire o non riuscire. Nelle seguenti sezioni viene illustrato cosa accade in ciascun caso.

Richiesta di invio riuscita

Se la richiesta a SES riesce, SES restituisce una risposta di esito positivo al mittente. Questo messaggio include l'ID messaggio, una stringa di caratteri che identifica in modo univoco la richiesta. È possibile utilizzare l'ID messaggio per trovare l'e-mail inviata o per tenere traccia dei problemi riscontrati durante l'invio (è necessario archiviare una propria mappatura tra un identificatore e l'ID messaggio SES che SES ritrasmette quando accetta l'e-mail). SES quindi assembla un messaggio e-mail in base ai parametri della richiesta, scansiona il messaggio per rilevare contenuti a rischio e virus, quindi lo invia su Internet tramite SMTP (Simple Mail Transfer Protocol). In genere, il messaggio viene inviato immediatamente: il primo tentativo di solito si verifica entro pochi millisecondi.

> **Note**
>
> Se SES accetta la richiesta del mittente e successivamente rileva che il messaggio contiene un virus, interrompe l'elaborazione del messaggio e non tenta di inviarlo al server di posta elettronica del destinatario.

Richiesta di invio non riuscita

Se la richiesta di invio di e-mail del mittente a SES non riesce, SES risponde al mittente con un messaggio di errore e rifiuta l'e-mail. La richiesta potrebbe non riuscire per vari motivi. Ad esempio, potrebbe non essere formattata correttamente o l'indirizzo e-mail potrebbe non essere stato verificato dal mittente.

Il metodo tramite il quale è possibile stabilire se la richiesta non è riuscita dipende dal modo in avviene la chiamata a SES. Di seguito sono elencati alcuni esempi di eccezioni ed errori che vengono restituiti:

- Se la chiamata a SES avviene tramite l'API di query (HTTPS) (`SendEmail` o `SendRawEmail`), le operazioni restituiscono un errore. Per ulteriori informazioni, consulta il Documento di riferimento API di Amazon Simple Notification Service.

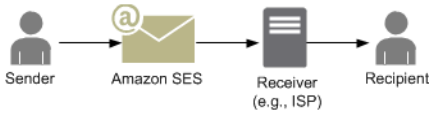
- In caso di uso di un SDK AWS per un linguaggio di programmazione che impiega le eccezioni, la chiamata a SES genera un'eccezione MessageRejectedException. (Il nome dell'eccezione può variare leggermente a seconda dell'SDK.)
- Se usi l'interfaccia SMTP, il mittente riceve un codice di risposta SMTP, ma il modo in cui l'errore viene trasmesso dipende dal client del mittente. Alcuni client possono visualizzare un codice di errore al contrario di altri.

Per informazioni sugli errori che possono verificarsi quando invii un'e-mail con SES, consulta Errori di invio di e-mail con Amazon SES.

Dopo l'invio di un e-mail da parte di Amazon SES

Se la richiesta del mittente a SES va a buon fine, SES invia l'e-mail e si verifica una delle seguenti situazioni:

- La consegna riesce e il destinatario non fa alcuna obiezione in merito all'e-mail: l'e-mail viene accettata dall'ISP e quest'ultimo consegna l'e-mail al destinatario. Nella figura seguente è illustrata una consegna completata.

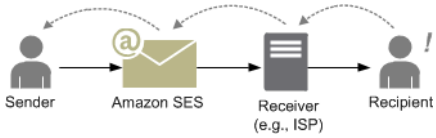


- Mancato recapito permanente: l'e-mail viene rifiutata dall'ISP a causa di una condizione persistente o da SES perché l'indirizzo e-mail è presente nel suo elenco di eliminazione. Un indirizzo e-mail si trova nell'elenco di eliminazione di SES se di recente è stato causa di un mancato recapito permanente per un cliente SES. Un hard bounce con un ISP può verificarsi perché l'indirizzo del destinatario non è valido. L'ISP invia una notifica di mancato recapito permanente a SES, che a sua volta invia notifica al mittente tramite e-mail o tramite il Servizio di notifica semplice Amazon (Amazon SNS), a seconda della configurazione del mittente. SES invia notifica al mittente dei mancati recapiti dell'elenco di eliminazione utilizzando lo stesso mezzo. Nella figura seguente è illustrato il percorso di un hard bounce da un ISP.

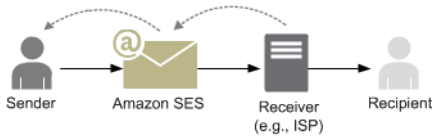
- E-mail non recapitata: l'ISP non è in grado di consegnare l'e-mail al destinatario a causa di una condizione temporanea, ad esempio l'ISP è troppo occupato per gestire la richiesta o la mailbox del destinatario è piena. Si verifica un soft bounce anche se il dominio non esiste. L'ISP invia una notifica di e-mail non recapitata a SES oppure, nel caso di un dominio inesistente, SES non è in

grado di trovare un server e-mail per il dominio. In entrambi i casi SES effettua altri tentativi per un periodo di tempo esteso. Se SES non è in grado di consegnare l'e-mail in questo periodo di tempo, invia una notifica di mancato recapito tramite e-mail o Amazon SNS. Se SES è in grado di recapitare l'e-mail al destinatario in un nuovo tentativo, la consegna è riuscita. Nella figura seguente è illustrato un soft bounce. In questo caso, SES prova ancora a inviare l'e-mail e l'ISP infine riesce a recapitarla al destinatario.

- Reclamo: l'e-mail viene accettata dall'ISP e recapitata al destinatario, ma il destinatario la considera spam e fa clic su un pulsante di tipo "Segnala come spam" per contrassegnarla come posta indesiderata nel proprio client e-mail. Se per SES è configurato un loop di feedback con l'ISP, viene inviata una notifica di reclamo a SES, che la inoltra al mittente. La maggior parte degli ISP omette l'indirizzo e-mail del destinatario che ha inviato il reclamo, pertanto nella notifica di reclamo da SES viene fornito al mittente un elenco di destinatari che potrebbero avere inviato il reclamo, in base ai destinatari del messaggio originale e all'ISP da cui SES ha ricevuto il reclamo. Nella figura che segue è illustrato il percorso di un reclamo.



- Risposta automatica: l'e-mail viene accettata dall'ISP, che la fa recapitare al destinatario. L'ISP quindi invia una risposta automatica, ad esempio un messaggio "fuori sede", a SES. SES inoltra quindi la notifica di risposta automatica al mittente. Nella figura seguente è illustrata una risposta automatica.



Assicurati che il programma abilitato per SES non faccia altri tentativi di inviare messaggi che generano una risposta automatica.

> **Tip**
>
> Puoi usare il simulatore di mailbox di SES per testare una consegna riuscita, un mancato recapito, un reclamo, un messaggio fuori sede o ciò che accade quando un indirizzo è

presente nell'elenco di eliminazione. Per ulteriori informazioni, consulta Utilizzo manuale del simulatore di mailbox.

Formato dell'e-mail in Amazon SES

Quando un client invia una richiesta ad Amazon SES, Amazon SES compone un messaggio e-mail compatibile con la specifica Internet Message Format (RFC 5322). Un'e-mail è costituita da un'intestazione, un corpo e una busta, come descritto di seguito.

- Intestazione: contiene le istruzioni di routing e le informazioni sul messaggio. Alcuni esempi sono l'indirizzo del mittente, l'indirizzo del destinatario, l'oggetto e la data. L'intestazione è simile alle informazioni nella parte superiore di una lettera postale, anche se può contenere molti altri tipi di informazioni, ad esempio il formato del messaggio.
- Corpo: contiene il testo del messaggio.
- Busta: contiene le informazioni di routing comunicate tra il client e il server di posta durante la sessione SMTP. Queste informazioni sono simili a quelle presenti su una busta postale. Le informazioni di routing della busta e-mail corrispondono generalmente, anche se non sempre, a quelle presenti nell'intestazione. Ad esempio, quando si invia una copia nascosta, l'indirizzo del destinatario effettivo (derivato dalla busta) non è lo stesso del campo del destinatario visualizzato nei client di posta elettronica del destinatario, che è derivato dall'intestazione.

Di seguito è illustrato un esempio semplice di e-mail. L'intestazione è seguita da una riga vuota, quindi dal corpo dell'e-mail. La busta non viene visualizzata perché viene comunicata tra il client e il server di posta durante la sessione SMTP, anziché essere una parte dell'e-mail.

```
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
```

Nelle seguenti sezioni vengono esaminate le intestazioni e i corpi delle e-mail e vengono identificate le informazioni che è necessario fornire quando si usa Amazon SES.

Intestazione dell'e-mail

Per ogni messaggio e-mail è presente una sola intestazione. Ogni riga dell'intestazione contiene un campo seguito da due punti, seguiti dal corpo. Quando si legge un'e-mail in un client di posta elettronica, sono in genere visualizzati i valori dei seguenti campi intestazione:

- To (A): gli indirizzi e-mail dei destinatari del messaggio.
- CC (Cc): gli indirizzi e-mail dei destinatari in copia nascosta del messaggio.
- From (Da): l'indirizzo e-mail da cui viene inviato il messaggio.
- Subject (Oggetto): un riepilogo dell'argomento del messaggio.
- Date (Data): la data e ora in cui l'e-mail viene inviata.

Esistono molti campi intestazione aggiuntivi che forniscono informazioni di routing e descrivono il contenuto del messaggio. Di solito i client di posta non visualizzano questi campi all'utente. Per un elenco completo dei campi di intestazione accettati da Amazon SES, consulta Campi di intestazione Amazon SES. Quando si usa Amazon SES, è particolarmente importante comprendere la differenza tra i campi di intestazione "From", "Reply-To" e "Return-Path". Come indicato in precedenza, l'indirizzo "From" corrisponde all'indirizzo e-mail del mittente del messaggio, mentre "Reply-To" e "Return-Path" sono:

- Reply-To: l'indirizzo e-mail a cui verranno inviate le risposte. Per impostazione predefinita, le risposte vengono inviate all'indirizzo e-mail del mittente originale.
- Return-Path: l'indirizzo e-mail a cui devono essere inviati i mancati recapiti e i reclami. "Return-Path" talvolta viene chiamato "envelope from", "envelope sender" o "MAIL FROM".

> **Note**
>
> Quando si usa Amazon SES, è sempre consigliabile impostare il parametro "Return-Path" in modo da rendersi conto del mancato recapito e intraprendere l'azione appropriata se necessario.

Per associare facilmente un messaggio non recapitato al rispettivo destinatario, è possibile utilizzare Variable Envelope Return Path (VERP). Con VERP, è possibile impostare un "Return-Path" diverso per ogni destinatario in modo che, se il messaggio viene rimbalzato, si capisce automaticamente da quale destinatario anziché dover aprire e analizzare il messaggio di mancato recapito.

Corpo dell'e-mail

Il corpo dell'e-mail contiene il testo del messaggio. Può essere inviato nei formati seguenti:

- HTML: se il client di posta del destinatario è in grado di interpretare l'HTML, il corpo può includere testo formattato e collegamenti ipertestuali
- Testo normale: se il client di posta del destinatario è basato su testo, il corpo non deve includere caratteri non stampabili.
- Sia HTML sia testo normale: quando si usano entrambi i formati per inviare lo stesso contenuto in un singolo messaggio, il client di posta del destinatario decide quale visualizzare, in base alle funzionalità di cui è dotato.

Se si invia un messaggio e-mail a un numero elevato di destinatari, è opportuno inviarlo in formato sia HTML sia di testo. Alcuni destinatari sono dotati di client di posta abilitati per HTML, pertanto possono fare clic sui collegamenti ipertestuali incorporati nel messaggio. Per i destinatari che usano i client di posta basati su testo sarà necessario includere gli URL che potranno copiare e aprire utilizzando un browser Web.

Informazioni dell'e-mail che è necessario fornire ad Amazon SES

Quando si invia un'e-mail con Amazon SES, le informazioni che è necessario fornire dipendono dal modo in cui si chiama Amazon SES. È possibile fornire una quantità minima di informazioni e fare in modo che le formattazioni vengano effettuate automaticamente in Amazon SES. Se invece si desidera eseguire un'operazione più avanzata, come inviare un allegato, è possibile fornire il messaggio in formato RAW. Nelle seguenti sezioni viene esaminato ciò che è necessario fornire

quando si invia un'e-mail utilizzando l'API Amazon SES, l'interfaccia SMTP Amazon SES o la console Amazon SES.

API Amazon SES

Se effettui una chiamata direttamente all'API Amazon SES, chiami `SendEmail` o l'API `SendRawEmail`. La quantità di informazioni che è necessario fornire dipende dall'API che si chiama.

- L'`SendEmail API` richiede di specificare solo un indirizzo di origine, un indirizzo di destinazione, l'oggetto del messaggio e il corpo del messaggio. Si possono fornire anche gli indirizzi "Reply-To". Quando si chiama questa API, Amazon SES assembla automaticamente un messaggio e-mail Multipurpose Internet Mail Extensions (MIME) in più parti formattato correttamente e ottimizzato per essere visualizzato dal software del client di posta. Per ulteriori informazioni, consultare Invio di e-mail formattate mediante l'API Amazon SES.
- L'API `SendRawEmail` fornisce agli utenti avanzati la possibilità di formattare e inviare i messaggi e-mail in formato RAW specificando le intestazioni, le parti MIME e i tipi di contenuto. `SendRawEmail` è utilizzata di solito dagli utenti avanzati. È necessario fornire il corpo del messaggio e tutti i campi intestazione specificati come obbligatori nella specifica Internet Message Format (RFC 5322). Per ulteriori informazioni, consultare Invio di e-mail non elaborate utilizzando l'API Amazon SES v2.

Se usi un SDK AWS per chiamare l'API Amazon SES, fornisci le informazioni elencate in precedenza alle funzioni corrispondenti (ad esempio, `SendEmail` e `SendRawEmail` per Java).

Per ulteriori informazioni sull'invio di e-mail mediante l'API Amazon SES, consulta Utilizzo dell'API Amazon SES per l'invio di e-mail.

Interfaccia SMTP di Amazon SES

Quando accedi ad Amazon SES attraverso l'interfaccia SMTP, la tua applicazione client SMTP assembla il messaggio, perciò le informazioni da fornire dipendono dall'applicazione utilizzata. Lo scambio SMTP tra un client e un server richiede, come minimo, un indirizzo di origine, un indirizzo di destinazione e i dati del messaggio.

Per ulteriori informazioni sull'invio di e-mail mediante l'interfaccia SMTP Amazon SES, consulta Utilizzo dell'interfaccia SMTP Amazon SES per inviare e-mail.

Console Amazon SES

Quando si invia un'e-mail utilizzando la console Amazon SES, la quantità di informazioni che è necessario fornire dipende dal fatto che si decida di inviare un messaggio e-mail formattato o in formato RAW.

- Per inviare un'e-mail formattata è necessario specificare un indirizzo di origine, un indirizzo di destinazione, l'oggetto del messaggio e il corpo del messaggio. Amazon SES assembla automaticamente un messaggio e-mail MIME in più parti, formattato correttamente e ottimizzato per essere visualizzato dal software del client di posta. Puoi anche specificare un campo di risposta e percorso di ritorno.
- Per inviare un messaggio e-mail in formato RAW, è necessario fornire l'indirizzo di origine, un indirizzo di destinazione e il contenuto del messaggio, che deve contenere il corpo del messaggio e tutti i campi di intestazione specificati come richiesto nella specifica Internet Message Format (RFC 5322).

Informazioni sulla capacità di recapitare e-mail in Amazon SES

Vuoi che i destinatari leggano le tue e-mail, le trovino valide e non le etichettino come spam. In altre parole, vuoi massimizzare la capacità di recapitare i messaggi, ovvero la percentuale di e-mail che raggiunge la posta in arrivo dei destinatari. Questo argomento descrive i concetti di efficienza del recapito che devi conoscere quando usi Amazon SES.

Per massimizzare la capacità di recapitare e-mail, è necessario capire i problemi di recapito delle e-mail, adottare in modo proattivo le misure necessarie per evitarli, rimanere informati sullo stato delle e-mail che si inviano, quindi migliorare il programma di invio di e-mail, se necessario, per aumentare ulteriormente le probabilità di riuscita delle consegne. Nelle seguenti sezioni vengono esaminati i concetti che sono alla base di queste fasi e viene illustrato in che modo Amazon SES aiuta a eseguire la procedura.

Comprensione dei problemi di consegna delle e-mail

Nella maggior parte dei casi, i messaggi vengono consegnati ai destinatari previsti. In alcune situazioni, tuttavia, la consegna potrebbe non riuscire o un destinatario potrebbe non voler ricevere l'e-mail che stai inviando. I mancati recapiti, i reclami e l'elenco di eliminazione sono correlati a questi problemi di consegna e sono descritti nelle seguenti sezioni.

Bounce (Mancato recapito)

Se il ricevitore del destinatario (ad esempio, un provider di posta elettronica) non riesce a consegnare il messaggio al destinatario, il ricevitore rimbalza il messaggio ad Amazon SES. Amazon SES quindi notifica il rimbalzo tramite e-mail o tramite Amazon Simple Notification Service (Amazon SNS), a seconda di come è configurato il sistema. Per ulteriori informazioni, consulta Impostazione delle notifiche degli eventi per Amazon SES.

Possono verificarsi hard bounce e soft bounce, come illustrato di seguito:

- Mancato recapito permanente: errore persistente di consegna di e-mail. Ad esempio, la mailbox non esiste. Amazon SES non effettua nuovi tentativi in caso di mancato recapito permanente, fatta eccezione degli errori di ricerca DNS. È consigliabile non effettuare tentativi ripetuti di consegna agli indirizzi e-mail che determinano l'errore di hard bounce.
- Soft bounce (e-mail non recapitata): errore temporaneo di consegna di e-mail. Ad esempio la mailbox è piena, sono presenti troppe connessioni (definito anche throttling (limitazione)) o la connessione scade. In caso di soft bounce (e-mail non recapitata), Amazon SES effettua tentativi ripetuti. Se comunque non si riesce a consegnare l'e-mail, Amazon SES smette di provare.

Amazon SES notifica gli hard bounce (mancato recapito permanente) e i soft bounce (e-mail non recapitata) per i quali non verranno fatti altri tentativi. Tuttavia, ai fini della frequenza di mancati recapiti e del parametro di mancati recapiti recuperati mediante la console Amazon SES o l'API `GetSendStatistics`, vengono conteggiati solo i mancati recapiti permanenti.

I mancati recapiti possono essere sincroni o asincroni. Un bounce sincrono si verifica quando i server e-mail del mittente e del ricevitore comunicano attivamente. Un bounce asincrono si verifica quando un ricevitore inizialmente accetta un messaggio e-mail per la consegna e successivamente non riesce a consegnarlo al destinatario.

Reclamo

La maggior parte dei programmi client e-mail offre la possibilità di classificare le e-mail come spam mediante un pulsante etichettato "Mark as Spam", o simile, che consente di spostare il messaggio in una cartella spam e di inoltrarlo al provider di posta elettronica. Inoltre, la maggior parte dei provider di posta elettronica ha un indirizzo per uso illecito (ad esempio abuse@example.net), a cui gli utenti possono inoltrare le e-mail indesiderate e richiedere che il provider di posta elettronica intraprenda un'azione per evitarle. In entrambi i casi il destinatario sta facendo un reclamo. Se il provider di posta elettronica conclude che sei uno spammer e Amazon SES ha un circuito di feedback impostato con il provider di posta elettronica, questo invierà nuovamente il reclamo ad Amazon SES. Quando Amazon SES riceve un reclamo di questo tipo, te lo inoltra tramite e-mail o utilizzando una notifica Amazon SNS, a seconda della configurazione del sistema. Per ulteriori informazioni, consulta Impostazione delle notifiche degli eventi per Amazon SES. È consigliabile non effettuare tentativi ripetuti di consegna agli indirizzi e-mail che generano reclami.

Elenco di eliminazione globale

L'elenco di eliminazione globale Amazon SES, di proprietà e gestito da SES per proteggere la reputazione degli indirizzi nel pool di IP condiviso SES, contiene gli indirizzi e-mail dei destinatari

che recentemente hanno provocato un mancato recapito permanente per un cliente SES. Se provi a inviare un'e-mail tramite SES a un indirizzo presente nell'elenco di eliminazione, la chiamata a SES riesce ma, invece di provare a inviare l'e-mail, SES la tratta come mancato recapito permanente. Come qualsiasi hard bounce, i mancati recapiti dell'elenco di eliminazione vengono conteggiati ai fini della quota di invio e della frequenza di mancato recapito. Un indirizzo e-mail può rimanere nell'elenco di eliminazione per un periodo massimo di 14 giorni. Se sei sicuro che l'indirizzo e-mail a cui stai tentando l'invio è valido, puoi sovrascrivere l'elenco di eliminazione globale assicurandoti che l'indirizzo non sia presente nell'elenco di eliminazione a livello di account e SES tenterà comunque la consegna. Tuttavia, se non si utilizza l'elenco di eliminazione a livello di account, in caso l'e-mail torni indietro, ci saranno ripercussioni sulla tua reputazione, ma senza che si verifichino mancati recapiti dovuti all'impossibilità di effettuare invii a quell'indirizzo e-mail. Per ulteriori informazioni sull'elenco di eliminazione a livello di account, consulta Utilizzo dell'elenco di eliminazione a livello di account di Amazon SES.

Prendi l'iniziativa

Uno dei principali problemi con l'e-mail su Internet riguarda le e-mail di massa non richieste (spam). I provider di posta elettronica adottano numerose misure per evitare che i propri clienti ricevano spam. Inoltre Amazon SES adotta misure per ridurre le probabilità che i provider di posta elettronica considerino la tua e-mail come spam. Amazon SES utilizza la verifica, l'autenticazione, i limiti di invio e il filtraggio del contenuto. Inoltre, Amazon SES mantiene una reputazione di affidabilità con i provider di posta elettronica e richiede agli utenti di inviare e-mail di alta qualità. Amazon SES esegue automaticamente alcune di queste operazioni (ad esempio il filtraggio del contenuto), mentre in altri casi fornisce gli strumenti (ad esempio l'autenticazione) o guida l'utente nell'esecuzione della procedura (quote di invio). Nelle sezioni seguenti vengono fornite ulteriori informazioni sui singoli concetti.

Verifica

Purtroppo uno spammer può falsificare l'intestazione di un'e-mail e contraffare l'indirizzo e-mail originale in modo da far credere che il messaggio provenga da una fonte diversa. Per preservare l'attendibilità tra i provider di posta elettronica e Amazon SES, Amazon SES deve verificare la reale identità dei mittenti. Pertanto, per proteggere la tua identità di invio, dovrai verificare tutti gli indirizzi e-mail da cui invii le e-mail tramite Amazon SES. Puoi verificare gli indirizzi e-mail utilizzando la console Amazon SES o l'API Amazon SES. Puoi anche verificare interi domini. Per ulteriori informazioni, consulta Creazione di un'identità dell'indirizzo e-mail e Creazione di un'identità dominio.

Se il tuo account si trova ancora nella sandbox Amazon SES, devi inoltre verificare tutti gli indirizzi dei destinatari, ad eccezione di quelli forniti dal simulatore di mailbox Amazon SES. Per informazioni

su come uscire dalla sandbox, consulta Richiedi l'accesso alla produzione (uscita dalla sandbox di Amazon SES). Per ulteriori informazioni sul simulatore di mailbox, consulta Utilizzo manuale del simulatore di mailbox.

Autenticazione

L'autenticazione è un altro modo per confermare al provider di posta elettronica la vera identità di un utente. Quando autentichi un'e-mail, dimostri di essere il proprietario dell'account e che le tue e-mail non sono state modificate durante il transito. In alcuni casi, i provider di posta elettronica rifiutano di inoltrare e-mail che non sono autenticate. Amazon SES supporta due metodi di autenticazione: Sender Policy Framework (SPF) e DomainKeys Identified Mail (DKIM). Per ulteriori informazioni, consulta Configurazione delle identità in Amazon SES.

Quote di invio

Se un provider di posta elettronica rileva picchi improvvisi non previsti nel volume o nella frequenza delle e-mail, potrebbe sospettare che sei uno spammer e bloccare le tue e-mail. Pertanto, ogni account Amazon SES dispone di un set di quote di invio. Queste quote limitano il numero di e-mail che è possibile inviare in un periodo di 24 ore e il numero che è possibile inviare al secondo. Queste quote di invio aiutano a proteggere la tua affidabilità con i provider di posta elettronica.

Se sei un nuovo utente, Amazon SES ti consente di inviare una piccola quantità di e-mail ogni giorno. Se la posta che invii è accettabile per i provider di posta elettronica, aumentiamo automaticamente questa quota. Nel corso del tempo, le quote di invio aumenteranno costantemente, in modo che sia possibile inviare maggiori quantità di e-mail con una frequenza maggiore. Inoltre puoi creare una pratica di aumento dei limiti di invio SES per richiedere ulteriori aumenti delle quote.

Per ulteriori informazioni sulle quote di invio e su come aumentarle, consulta Gestione dei limiti di invio di Amazon SES.

Filtraggio del contenuto

Molti provider di posta elettronica usano il filtraggio del contenuto per stabilire se le e-mail in entrata sono spam. I filtri cercano contenuto a rischio e bloccano le e-mail se corrispondono al profilo dello spam. Anche Amazon SES usa i filtri del contenuto. Quando la tua applicazione invia una richiesta ad Amazon SES, Amazon SES assembla un messaggio e-mail a tuo nome, quindi analizza l'intestazione e il corpo del messaggio per stabilire se includono contenuto che i provider di posta elettronica potrebbero interpretare come spam. Se, in base ai filtri del contenuto usati da Amazon SES, i tuoi messaggi rimandano allo spam, la tua reputazione con Amazon SES viene compromessa.

Amazon SES inoltre analizza tutti i messaggi alla ricerca di virus. Se un messaggio contiene un virus, Amazon SES non tenta di consegnarlo al server di posta del destinatario.

Reputazione

Quando si tratta di inviare e-mail, è fondamentale la reputazione, ovvero il grado di fiducia che un indirizzo IP, un indirizzo e-mail o un dominio di invio non sia fonte di spam. Amazon SES mantiene un'ottima reputazione con i provider di posta elettronica, che in questo modo consegnano le tue e-mail alle caselle di posta in arrivo dei destinatari. Analogamente, è necessario mantenere una reputazione di fiducia con Amazon SES. Puoi creare la tua reputazione con Amazon SES inviando contenuto di alta qualità. Quando si invia contenuto di alta qualità, la reputazione diventa più affidabile nel tempo e Amazon SES aumenta le quote di invio. Un numero eccessivo di mancati recapiti (bounce) e reclami influisce negativamente sulla tua reputazione e può causare la riduzione delle quote di invio per il tuo account da parte di Amazon SES o la chiusura del tuo account Amazon SES.

Uno dei modi per aiutare a mantenere la tua reputazione è quello di utilizzare il simulatore di mailbox quando esegui il test del sistema, anziché inviare agli indirizzi e-mail creati. Le e-mail inviate al simulatore di mailbox non contano ai fini dei parametri di reclamo e mancato recapito. Per ulteriori informazioni sul simulatore di mailbox, consulta Utilizzo manuale del simulatore di mailbox.

E-mail di alta qualità

Si tratta di e-mail che per i destinatari sono importanti e che pertanto desiderano ricevere. Ogni destinatario attribuisce più importanza a un tipo di e-mail rispetto a un altro: offerte, conferme di ordine, ricevute, newsletter e così via. Infine, la tua capacità di recapitare messaggi si basa sulla qualità delle e-mail che invii, in quanto i provider di posta elettronica bloccano le e-mail che considerano di qualità scadente.

Rimani aggiornato

Se le tue consegne non vanno a buon fine, i destinatari si lamentano delle tue e-mail o Amazon SES consegna un'e-mail al server di posta di un destinatario, Amazon SES ti permette di risalire alla causa del problema fornendo notifiche e consentendo di monitorare facilmente le statistiche di utilizzo.

Notifiche

Quando un'e-mail viene rimbalzata al mittente, il provider di posta elettronica invia notifica ad Amazon SES e Amazon SES invia notifica a te. Amazon SES notifica gli hard bounce (mancato recapito permanente) e i soft bounce (e-mail non recapitata) per i quali non effettuerà altri tentativi. Inoltre, molti provider di posta elettronica inoltrano i reclami e Amazon SES imposta circuiti di feedback dei

reclami con i principali provider di posta elettronica, pertanto non dovrai occupartene tu. Amazon SES può notificare mancati recapiti, reclami e consegne andate a buon fine in due modi: puoi impostare il tuo account in modo che riceva notifiche tramite Amazon SNS oppure puoi ricevere notifiche via e-mail (solo messaggi non recapitati e reclami). Per ulteriori informazioni, consulta Impostazione delle notifiche degli eventi per Amazon SES.

Statistiche di utilizzo

Amazon SES fornisce le statistiche di utilizzo, grazie alle quali puoi visualizzare le consegne non riuscite e determinare e risolvere le cause principali. Puoi visualizzare le statistiche di utilizzo mediante la console Amazon SES o chiamando l'API Amazon SES. Puoi visualizzare tutti i reclami, le consegne, i mancati recapiti (bounce) e le e-mail infette da virus rifiutate, nonché le quote di invio per essere sicuro di rispettarle.

Miglioramento del programma di invio di e-mail

Se si verificano numerosi casi di mancati recapiti e reclami, è ora di riesaminare la tua strategia di invio di e-mail. Ricorda che un numero eccessivo di mancati recapiti, reclami e tentativi di inviare e-mail di qualità scadente costituiscono un uso illecito ed espongono il tuo Account AWS al rischio di chiusura. Infine, devi usare Amazon SES per inviare messaggi e-mail di alta qualità e inviare e-mail solo a destinatari che desiderano riceverle.

Consegna "At-Least-Once"

Amazon SES archivia copie dei messaggi su più server per ridondanza e disponibilità elevata. In rare occasioni, uno dei server che memorizza una copia di un messaggio potrebbe non essere disponibile quando ricevi o elimini un messaggio.

In tal caso, la copia del messaggio non viene eliminata sul server non disponibile, e potresti ricevere di nuovo la copia del messaggio quando ricevi i messaggi. Progetta le tue applicazioni affinché siano idempotent (non devono essere condizionate negativamente quando elaborano lo stesso messaggio più di una volta).

Best practice per inviare e-mail utilizzando Amazon SES

Il modo in cui gestisci le comunicazioni e-mail con i tuoi clienti viene chiamato programma e-mail. Vi sono diversi fattori che possono determinare il successo o il fallimento del programma e-mail e, inizialmente, possono sembrare confusi o enigmatici. Tuttavia, comprendendo il modo in cui le e-mail vengono consegnate e seguendo alcune best practice, puoi aumentare le probabilità che le tue e-mail raggiungano le caselle di posta in arrivo dei clienti.

Argomenti

Parametri di riuscita del programma e-mail

Vi sono diversi parametri che consentono di misurare la riuscita del tuo programma e-mail.

Questa sezione contiene informazioni relative ai parametri seguenti:

- Mancati recapiti
- Reclami
- Qualità dei messaggi

Mancati recapiti

Un mancato recapito (bounce) si verifica quando un'e-mail non può essere consegnata al destinatario previsto. I mancati recapiti possono essere classificati come hard bounce (mancato recapito permanente) e soft bounce (e-mail non recapitata). Un hard bounce si verifica quando l'e-mail non può essere consegnata a causa di un problema permanente, ad esempio quando un indirizzo e-mail non esiste. Un soft bounce si verifica quando un problema temporaneo impedisce la consegna di un'e-mail. I soft bounce (e-mail non recapitata) possono verificarsi quando la casella di posta in arrivo di un destinatario è piena oppure quando il server ricevente non è temporaneamente disponibile. Amazon SES gestisce i soft bounce (e-mail non recapitata) cercando di consegnare nuovamente le e-mail non recapitate per un determinato periodo di tempo.

È essenziale monitorare il numero di hard bounce nel tuo programma e-mail e rimuovere gli indirizzi che li provocano dal tuo elenco di destinatari. Quando i ricevitori di e-mail rilevano una percentuale elevata di hard bounce, presuppongono che non tu non conosca bene i tuoi destinatari. Di conseguenza, una percentuale elevata di hard bounce può influire negativamente sull'efficienza del recapito dei tuoi messaggi e-mail.

Le seguenti linee guida possono aiutarti a evitare i mancati recapiti e migliorare la tua reputazione di mittente:

- Prova a mantenere la percentuale di hard bounce al di sotto del 5%. Più è ridotto il numero di hard bounce nel tuo programma e-mail, più gli ISP tenderanno a considerare i tuoi messaggi

come legittimi e di valore. Questa percentuale deve essere considerata un obiettivo ragionevole e raggiungibile, ma non rappresenta una regola valida universalmente per tutti gli ISP.

- Non noleggiare o acquistare mai elenchi di indirizzi e-mail. Questi elenchi potrebbero contenere un numero elevato di indirizzi non validi, la qual cosa potrebbe causare un notevole incremento della tua percentuale di hard bounce. Inoltre, questi elenchi potrebbero contenere spam trap, cioè indirizzi e-mail specificamente utilizzati per individuare mittenti illegittimi. Se i tuoi messaggi arrivano in una spam trap, le tue percentuali di consegna e la reputazione di mittente potrebbe venirne irrimediabilmente compromessi.
- Mantieni il tuo elenco aggiornato. Se non hai inviato e-mail ai tuoi destinatari per un lungo periodo di tempo, prova a verificare lo stato dei tuoi clienti attraverso altri mezzi, come l'attività di accesso al tuo sito Web o lo storico degli acquisti.
- Se non disponi di un metodo per verificare lo stato dei clienti, valuta la possibilità di inviare un messaggio e-mail di riconquista. Un tipico messaggio di riconquista afferma che non senti il cliente da qualche tempo e lo incoraggi a confermare che desidera ancora ricevere le tue e-mail. Dopo l'invio di un messaggio e-mail di riconquista, rimuovi dagli elenchi tutti i destinatari che non hanno risposto.

Quando ricevi mancati recapiti, è fondamentale che tu reagisca in modo appropriato osservando le seguenti regole:

- In caso di hard bounce, rimuovi immediatamente dai tuoi elenchi l'indirizzo che lo ha provocato. Non tentare di ripetere l'invio di messaggi a indirizzi che hanno provocato un hard bounce. Gli hard bounce ripetuti si sommano e finiscono con il danneggiare la tua reputazione presso l'ISP del destinatario.
- Verifica che l'indirizzo che stai utilizzando per ricevere notifiche di mancato recapito sia in grado di ricevere e-mail. Per ulteriori informazioni sulla configurazione di notifiche di mancato recapito e reclamo, consulta Impostazione delle notifiche degli eventi per Amazon SES.
- Se le tue e-mail in entrata arrivano da un ISP, anziché tramite i tuoi server interni, un afflusso di notifiche di mancato recapito può arrivare nella cartella spam o essere eliminato del tutto. Idealmente non dovresti utilizzare un indirizzo e-mail ospitato per ricevere i mancati recapiti. Se è inevitabile, tuttavia, controlla spesso la cartella spam e non contrassegnare come spam i messaggi di mancato recapito. In Amazon SES puoi specificare l'indirizzo a cui inviare le notifiche di mancato recapito.
- Di solito, un mancato recapito fornisce l'indirizzo della casella postale che ha rifiutato la consegna. Tuttavia, se hai bisogno di dati più granulari per mappare l'indirizzo di un destinatario a una

determinata campagna e-mail, includi un campo X-header con un valore che puoi rintracciare all'interno del sistema di monitoraggio interno. Per ulteriori informazioni, consulta Campi di intestazione Amazon SES.

Reclami

Un reclamo si verifica quando il destinatario di un messaggio e-mail sceglie il pulsante "Contrassegna come spam" (o equivalente) nel client e-mail Web. Se accumuli un numero elevato di questi reclami, l'ISP presuppone che tu stia inviando spam. Questo ha un impatto negativo sul tuo tasso di efficienza del recapito e sulla tua reputazione di mittente. Alcuni ISP, ma non tutti, inviano una notifica quando un viene segnalato un reclamo; questo processo è noto come circuito di feedback. Amazon SES inoltra automaticamente i reclami degli ISP che offrono circuiti di feedback.

Le seguenti linee guida ti possono aiutare a evitare i reclami e migliorare la tua reputazione di mittente:

- Prova a mantenere la percentuale di reclami al di sotto dello 0,1%. Più è ridotto il numero di reclami nel tuo programma e-mail, più gli ISP tenderanno a considerare i tuoi messaggi come legittimi e di valore. Questa percentuale deve essere considerata un obiettivo ragionevole e raggiungibile, ma non rappresenta una regola valida universalmente per tutti gli ISP.
- Se un cliente presenta un reclamo su un messaggio e-mail di marketing, devi immediatamente interrompere l'invio di e-mail di marketing a quel cliente. Tuttavia, se il programma e-mail include anche altri tipi di e-mail (ad esempio e-mail di notifica o transazionali), può essere accettabile continuare a inviare questi tipi di messaggi al destinatario che ha presentato il reclamo.
- Come per gli hard bounce, se disponi di un elenco a cui non invii e-mail da un po' di tempo, assicurati che i destinatari comprendano il motivo per cui ricevono i tuoi messaggi. È consigliabile inviare un messaggio di benvenuto ricordando loro chi sei e perché li contatti.

Quando ricevi reclami, è fondamentale che tu reagisca in modo appropriato osservando le seguenti regole:

- Verifica che l'indirizzo che stai utilizzando per ricevere notifiche di reclamo sia in grado di ricevere e-mail. Per ulteriori informazioni sulla configurazione di notifiche di mancato recapito e reclamo, consulta Impostazione delle notifiche degli eventi per Amazon SES.
- Assicurati che le notifiche di reclamo non siano contrassegnate come spam dal tuo ISP o sistema di posta.

- Le notifiche di reclamo in genere contengono il corpo dell'e-mail; tali notifiche sono diverse dalle notifiche di mancato recapito, che in genere includono solo le intestazioni dell'e-mail. Tuttavia, nelle notifiche di reclamo l'indirizzo e-mail del soggetto che ha presentato il reclamo viene rimosso. Usa campi X-header personalizzati o identificatori speciali incorporati nel corpo dell'e-mail in modo da identificare l'indirizzo e-mail che ha presentato il reclamo. Questa tecnica è un modo semplice per identificare gli indirizzi che hanno presentato reclamo in modo che sia possibile rimuoverli dai tuoi elenchi di destinatari.

Qualità dei messaggi

I ricevitori e-mail utilizzano filtri di contenuto per rilevare determinati attributi nei messaggi allo scopo di determinare se il messaggio è legittimo. Questi filtri esaminano automaticamente il contenuto dei messaggi per identificare i tratti comuni di messaggi indesiderati e dannosi. Amazon SES usa tecnologie di filtro dei contenuti che facilitano l'individuazione e il blocco dei messaggi che contengono malware prima dell'invio.

Se i filtri di contenuto del ricevitore e-mail determina che il tuo messaggio contiene le caratteristiche di spam o e-mail dannosa, il messaggio verrà molto probabilmente contrassegnato e non inviato alle caselle di posta in arrivo dei destinatari.

Quando progetti la tua e-mail, ricorda quanto segue:

- I moderni filtri di contenuto si adattano e cambiano continuamente in modo intelligente. Non si basano su un set di regole predefinito. Servizi di terza parte, come ReturnPath o Litmus possono facilitare l'identificazione di contenuto nelle tue e-mail che potrebbe attivare i filtri di contenuto.
- Se il messaggio e-mail contiene link, controlla che gli URL dei link non siano presenti in elenchi DNSBL (DNS-based Blackhole Lists) come quelli disponibili su URIBL.com e SURBL.org.
- Evita di utilizzare abbreviazioni dei collegamenti. I mittenti malintenzionati possono utilizzare abbreviazioni per nascondere la destinazione effettiva di un collegamento. Quando gli ISP notano l'uso di servizi di abbreviazione dei collegamenti, anche i più attendibili, per scopi illeciti, possono negare l'accesso anche a questi servizi. Se la tua e-mail contiene un collegamento a un servizio di abbreviazione dei collegamenti che è stato aggiunto a un elenco di servizi rifiutati, non raggiungerà le caselle di posta in arrivo dei tuoi clienti, a pregiudizio del successo della tua campagna.
- Prova ogni collegamento nella tua e-mail per verificare che punti alla pagina desiderata.
- Assicurati che il tuo sito Web includa l'informativa sulla privacy e le condizioni d'uso e che tali documenti siano aggiornati. È buona norma inserire un link a questi documenti in ciascuna e-mail

inviata. Fornire i collegamenti a questi documenti dimostra che non hai nulla da nascondere ai clienti e questo può favorire lo sviluppo di una relazione di fiducia.

- Se intendi inviare contenuti ad alta frequenza (ad esempio messaggi con "le offerte del giorno"), assicurati che il contenuto dell'e-mail sia diverso per ogni distribuzione. Quando invii messaggi con alta frequenza, è importante che siano tempestivi e pertinenti, piuttosto che ripetitivi e fastidiosi.

Suggerimenti e best practice

Anche quando operi nell'interesse dei clienti è possibile che si verifichino situazioni che impattano sull'efficienza del recapito dei tuoi messaggi. Le seguenti sezioni contengono suggerimenti utili ad assicurare che le tue comunicazioni e-mail raggiungano i destinatari previsti.

Suggerimenti generali

- Mettiti al posto del cliente. Chiediti se il messaggio che stai inviando è qualcosa che vorresti ricevere nella tua casella di posta. Se la risposta non è decisamente affermativa, probabilmente non dovresti inviarlo.
- Alcuni settori hanno una reputazione di pratiche di invio di e-mail di scarsa qualità o addirittura dannose. Se operi nei seguenti settori, devi monitorare la tua reputazione in modo rigoroso e risolvere subito i problemi:
  - Ipoteche e mutui
  - Credito
  - Prodotti farmaceutici e integratori
  - Alcol e tabacco
  - Intrattenimento per adulti
  - Gioco d'azzardo e scommesse
  - Programmi di lavoro a domicilio

Considerazioni sui domini e gli indirizzi "From"

- Pensa attentamente agli indirizzi da cui invii le e-mail. L'indirizzo "From" è una delle prime informazioni visualizzate dai destinatari e, di conseguenza, può lasciare una prima impressione durevole. Inoltre, alcuni ISP associano la tua reputazione al tuo indirizzo "From".
- Considera l'utilizzo di sottodomini per i diversi tipi di comunicazioni. Ad esempio, supponi di inviare e-mail dal dominio example.com e di voler inviare sia messaggi transazionali che di

marketing. Piuttosto che inviare tutti i messaggi da example.com, invia i messaggi di marketing da un sottodominio come marketing.example.com e i messaggi transazionali da un sottodominio come orders.example.com. Sottodomini univoci sviluppano la propria reputazione. L'utilizzo di sottodomini riduce il rischio di danni alla reputazione se, ad esempio, le comunicazioni di marketing arrivano in una spam trap o attivano un filtro di contenuto.

- Se prevedi di inviare un numero elevato di messaggi, non inviarli da un indirizzo basato su ISP, come sender@hotmail.com. Se un ISP nota un grande volume di messaggi provenienti da sender@hotmail.com, li tratta in modo diverso rispetto a un messaggio e-mail che proviene da un dominio di invio di e-mail in uscita di tua proprietà.
- Collabora con il registrar di domini per assicurare che le informazioni WHOIS del tuo dominio siano accurate. Mantenere un record WHOIS veritiero e aggiornato dimostra che tieni alla trasparenza e consente agli utenti di determinare rapidamente se il tuo dominio è legittimo.
- Evitare di utilizzare un indirizzo no-reply, ad esempio no-reply@example.com, come indirizzo del mittente o "Reply-to". L'utilizzo di un indirizzo e-mail no-reply@ indica chiaramente ai destinatari che non stai offrendo loro un modo per contattarti e che non ti interessa il loro feedback.

Autenticazione

- Autentica il tuo dominio con SPF e SenderID. Questi metodi di autenticazione confermano ai destinatari che ogni e-mail inviata da te proviene effettivamente dal dominio dichiarato.
- Firma la tua posta in uscita con DKIM. Questa fase conferma ai destinatari che il contenuto non è stato modificato nel transito tra mittente e ricevitore.
- Puoi testare le tue impostazioni di autenticazione sia per SPF che DKIM inviando un'e-mail a un indirizzo basato su ISP di tua proprietà, ad esempio un account Gmail o Hotmail personale, quindi esaminando le intestazioni del messaggio. Le intestazioni indicano se i tuoi tentativi di autenticare e firmare il messaggio sono riusciti.

Creazione e gestione degli elenchi

- Implementa una strategia con doppio consenso. Quando gli utenti si registrano per ricevere e-mail da te, invia loro un messaggio con un collegamento di conferma e non iniziare a inviare e-mail finché non confermano il loro indirizzo facendo clic su questo collegamento. Una strategia con doppio consenso aiuta a ridurre il numero di hard bounce risultanti da errori ortografici.

- Quando raccogli gli indirizzi e-mail con un modulo Web, esegui almeno una convalida di base quando gli indirizzi vengono inoltrati. Ad esempio, assicurati che gli indirizzi raccolti siano in formato corretto (recipient@example.com) e che si riferiscano a domini con record MX validi.
- Utilizza cautela quando consenti il passaggio non verificato di input definito dall'utente ad Amazon SES. Le registrazioni ai forum e l'invio di moduli presentano rischi speciali perché il contenuto è completamente generato dagli utenti e gli spammer possono compilare i moduli inserendo propri contenuti. È tua responsabilità assicurarti di inviare solo e-mail con contenuti di alta qualità.
- È altamente improbabile che un alias standard (ad esempio postmaster@, abuse@ o noc@) effettui la registrazione per ricevere le tue e-mail intenzionalmente. Assicurati di inviare messaggi solo a persone reali che desiderano effettivamente riceverli. Questa regola è particolarmente valida per gli alias standard, che sono abitualmente riservati per funzioni di sorveglianza e-mail. Questi alias possono essere aggiunti al tuo elenco con intento malevolo, come una forma di sabotaggio, per danneggiare la tua reputazione.

Conformità

- Sii consapevole delle leggi e dei regolamenti anti-spam e sull'e-mail marketing in vigore nei paesi e nelle regioni in cui invii le e-mail. Sei tenuto a garantire la conformità delle e-mail che invii a tali leggi. Questa guida non riguarda le suddette leggi, è perciò importante informarsi in modo specifico. Per un elenco di leggi, consulta la voce relativa alla legislazione anti-spam per paese su Wikipedia.
- Consulta sempre un avvocato per ottenere adeguati pareri legali.

Utilizzo di Amazon SES con un AWS SDK

AWS I kit di sviluppo software (SDK) sono disponibili per molti linguaggi di programmazione più diffusi. Ogni SDK fornisce un'API, esempi di codice, e documentazione che facilitano agli sviluppatori la creazione di applicazioni nel loro linguaggio preferito.

Documentazione sugli SDK	Esempi di codice
AWS SDK for C++	AWS SDK for C++ esempi di codice
AWS CLI	AWS CLI esempi di codice
AWS SDK for Go	AWS SDK for Go esempi di codice

Documentazione sugli SDK	Esempi di codice
AWS SDK for Java	AWS SDK for Java esempi di codice
AWS SDK for JavaScript	AWS SDK for JavaScript esempi di codice
SDK AWS for Kotlin	SDK AWS for Kotlin esempi di codice
AWS SDK for .NET	AWS SDK for .NET esempi di codice
AWS SDK for PHP	AWS SDK for PHP esempi di codice
AWS Tools for PowerShell	Strumenti per esempi di PowerShell codice
AWS SDK for Python (Boto3)	AWS SDK for Python (Boto3) esempi di codice
AWS SDK for Ruby	AWS SDK for Ruby esempi di codice
AWS SDK for Rust	AWS SDK for Rust esempi di codice
SDK AWS per SAP ABAP	SDK AWS per SAP ABAP esempi di codice
SDK AWS per Swift	SDK AWS per Swift esempi di codice

Per esempi specifici di Amazon SNS, consulta la sezione Esempi di codice per Amazon SES con SDK AWS.

> **Esempio di disponibilità**
>
> Non riesci a trovare quello che ti serve? Richiedi un esempio di codice utilizzando il link Provide feedback (Fornisci un feedback) nella parte inferiore di questa pagina.

Nozioni di base su Amazon Simple Storage Service

Questo capitolo ti guida attraverso le attività necessarie per la configurazione iniziale di Amazon SES e tutorial per aiutarti a muovere i primi passi.

Argomenti

- Impostazione di Amazon Simple Email Service
- Migrazione ad Amazon SES da un'altra soluzione di invio di e-mail
- Richiedi l'accesso alla produzione (uscita dalla sandbox di Amazon SES)

Impostazione di Amazon Simple Email Service

Prima di iniziare a utilizzare Amazon SES, completa le seguenti attività.

Attività

- Iscriviti per AWS
- Configurazione dell'account SES
- Concessione dell'accesso programmatico (per interagire con SES al di fuori della console)
- Scarica un AWS SDK (per utilizzare le API SES)

Iscriviti per AWS

Se non ne hai uno Account AWS, completa i seguenti passaggi per crearne uno.

Per iscriverti a un Account AWS

1. Apri la pagina all'indirizzo https://portal.aws.amazon.com/billing/signup.
2. Segui le istruzioni online.

   Nel corso della procedura di registrazione riceverai una telefonata, durante la quale sarà necessario inserire un codice di verifica attraverso la tastiera del telefono.

   Quando ti iscrivi a un Account AWS, Utente root dell'account AWSviene creato un. L'utente root dispone dell'accesso a tutte le risorse e tutti i Servizi AWS nell'account. Come procedura consigliata in materia di sicurezza, assegnate l'accesso amministrativo a un utente e utilizzate solo l'utente root per eseguire attività che richiedono l'accesso da parte dell'utente root.

Configurazione dell'account SES

Inizia a usare SES verificando un indirizzo e-mail e un dominio di invio in modo da poter iniziare a inviare e-mail tramite SES e richiedere l'accesso alla produzione per il tuo account utilizzando la procedura guidata di configurazione dell'account SES.

Utilizzo della procedura guidata di configurazione dell'account SES per configurare l'account

1. Accedi AWS Management Console e apri la console Amazon SES all'indirizzo https://console.aws.amazon.com/ses/.
2. Seleziona Per iniziare dalla home page della console SES e la procedura guidata ti guiderà attraverso le fasi di configurazione dell'account SES.

La procedura guidata di configurazione dell'account SES verrà visualizzata solo se non hai ancora creato alcuna identità (indirizzo e-mail o dominio) in SES.

Concessione dell'accesso programmatico (per interagire con SES al di fuori della console)

Gli utenti hanno bisogno di un accesso programmatico se vogliono interagire con l' AWS AWS Management Console esterno di. Il modo per concedere l'accesso programmatico dipende dal tipo di utente che accede. AWS

Per fornire agli utenti l'accesso programmatico, scegli una delle seguenti opzioni.

Quale utente necessita dell'accesso programmatico?	Per	Come
Identità della forza lavoro (Utenti gestiti nel centro identità IAM)	Utilizza credenziali temporane e per firmare le richieste programmatiche agli AWS CLI AWS SDK o alle API. AWS	Segui le istruzioni per l'interfa ccia che desideri utilizzare. • Per la AWS CLI, consulta Configurazione dell'uso AWS IAM Identity Center nella Guida AWS CLI per l'utente.AWS Command Line Interface

Quale utente necessita dell'accesso programmatico?	Per	Come
		• Per AWS SDK, strumenti e AWS API, consulta l'autenticazione IAM Identity Center nella Guida di riferimento agli AWS SDK e agli strumenti.
IAM	Utilizza credenziali temporane e per firmare le richieste programmatiche agli SDK o alle API AWS CLI. AWS AWS	Segui le istruzioni in Uso delle credenziali temporanee con AWS risorse nella Guida per l'utente IAM.
IAM	(Non consigliato) Utilizza credenziali a lungo termine per firmare le richieste programmatiche agli AWS CLI AWS SDK o alle API. AWS	Segui le istruzioni per l'interfa ccia che desideri utilizzare. • Per la AWS CLI, consulta Autenticazione tramite credenziali utente IAM nella Guida per l'utente.AWS Command Line Interface • Per gli AWS SDK e gli strumenti, consulta Autenticazione tramite credenziali a lungo termine nella Guida di riferimen to agli SDK e agli AWS strumenti. • Per le AWS API, consulta Gestione delle chiavi di accesso per gli utenti IAM nella Guida per l'utente IAM.

Scarica un AWS SDK (per utilizzare le API SES)

Per chiamare le API SES senza dover gestire dettagli di basso livello come l'assemblaggio di richieste HTTP non elaborate, puoi utilizzare un SDK. AWS Gli AWS SDK forniscono funzioni e tipi di dati che racchiudono le funzionalità di SES e di altri servizi. AWS Per scaricare un AWS SDK, accedi agli SDK. Dopo aver scaricato l'SDK, crea un file di credenziali condiviso e specifica le tue chiavi di accesso. AWS

Migrazione ad Amazon SES da un'altra soluzione di invio di e-mail

Questo argomento descrive una panoramica delle fasi da seguire per spostare la soluzione di invio di messaggi e-mail ad Amazon SES da una soluzione ospitata in locale o in un'istanza Amazon EC2.

Argomenti in questa sezione:

- Fase 1: Verifica del dominio
- Fase 2: Richiesta dell'accesso di produzione
- Fase 3. Configurazione dei sistemi di autenticazione del dominio
- Fase 4. Generazione delle credenziali SMTP
- Fase 5. Connessione a un endpoint SMTP
- Passaggi successivi

Fase 1: Verifica del dominio

Prima di poter utilizzare Amazon SES per inviare e-mail, è necessario verificare le identità da cui pensi di inviare e-mail. In Amazon SES, un'identità può essere un indirizzo e-mail o un intero dominio. Una volta verificato un dominio, puoi usare Amazon SES per inviare e-mail da qualsiasi indirizzo all'interno di tale dominio. Per ulteriori informazioni sulla verifica dei domini, consulta Creazione di un'identità dominio.

Fase 2: Richiesta dell'accesso di produzione

Quando inizi a utilizzare Amazon SES per la prima volta, il tuo account si trova in un ambiente sandbox. Mentre l'account si trova nella sandbox, puoi inviare e-mail solo agli indirizzi verificati. Inoltre, si applicano restrizioni sul numero di messaggi che è possibile inviare al giorno e al secondo. Per ulteriori informazioni sulla richiesta di accesso di produzione, consulta Richiedi l'accesso alla produzione (uscita dalla sandbox di Amazon SES).

Fase 3. Configurazione dei sistemi di autenticazione del dominio

Puoi configurare il dominio per l'utilizzo di sistemi di autenticazione quali DKIM e SPF. Questa fase è tecnicamente facoltativa. Tuttavia, impostando DKIM o SPF (o entrambi) per il tuo dominio, puoi migliorare l'efficienza del recapito delle tue e-mail e aumentare la fiducia dei tuoi clienti. Per ulteriori informazioni sulla configurazione di SPF, consulta Autenticazione delle e-mail con SPF in Amazon SES. Per ulteriori informazioni sulla configurazione di DKIM, consulta Autenticazione delle e-mail con DKIM in Amazon SES.

Fase 4. Generazione delle credenziali SMTP

Se pensi di inviare e-mail utilizzando un'applicazione che usa SMTP, devi generare le credenziali SMTP. Le credenziali SMTP sono diverse dalle normali credenziali AWS . Queste credenziali sono inoltre uniche in ogni regione. AWS Per ulteriori informazioni su come generare le credenziali SMTP, consulta Richiesta delle credenziali SMTP Amazon SES.

Fase 5. Connessione a un endpoint SMTP

Se usi un agente di trasferimento messaggi, ad esempio postfix o sendmail, devi aggiornare la configurazione per tale applicazione in modo da fare riferimento a un endpoint SMTP Amazon SES. Per un elenco completo degli endpoint SMTP, consulta Connessione a un endpoint SMTP Amazon SES. Si noti che le credenziali SMTP create nel passaggio precedente sono associate a una regione specifica. AWS È necessario connettersi all'endpoint SMTP nella regione in cui sono state create le credenziali SMTP.

Passaggi successivi

A questo punto, sei pronto per iniziare a inviare e-mail utilizzando Amazon SES. Tuttavia, ci sono alcuni passaggi facoltativi che puoi eseguire.

- È possibile creare i set di configurazione, che sono insiemi di regole che vengono applicate ai messaggi e-mail inviati. Ad esempio, puoi utilizzare i set di configurazione per specificare dove vengono inviate le notifiche quando viene recapitato un messaggio e-mail, quando un destinatario apre un messaggio o fa clic su un collegamento al suo interno, quando un messaggio e-mail restituisce un mancato recapito e quando un destinatario contrassegna l'e-mail come posta indesiderata. Per ulteriori informazioni, consulta Utilizzo dei set di configurazione in Amazon SES.
- Quando invii un'e-mail tramite Amazon SES, è importante monitorare i manchi recapiti e i reclami relativi al tuo account. Amazon SES include una pagina della console dei parametri di reputazione che puoi utilizzare per tenere traccia dei manchi recapiti e dei reclami relativi al tuo account.

Per ulteriori informazioni, consulta Utilizzo dei parametri sulla reputazione per tenere traccia delle percentuali di mancati recapiti e reclami. Puoi anche creare CloudWatch allarmi che ti avvisano quando queste tariffe diventano troppo alte. Per ulteriori informazioni sulla creazione di CloudWatch allarmi, consulta. Creazione di allarmi di monitoraggio della reputazione tramite CloudWatch

- I clienti che inviano un numero elevato di e-mail o coloro che vogliono semplicemente avere il pieno controllo sulla reputazione dei loro indirizzi IP, possono noleggiare indirizzi IP dedicati con un supplemento mensile. Per ulteriori informazioni, consulta Indirizzi IP dedicati per Amazon SES.

Richiedi l'accesso alla produzione (uscita dalla sandbox di Amazon SES)

Per prevenire frodi e usi illeciti e per aiutare a proteggere la tua reputazione come mittente, applichiamo alcune limitazioni ai nuovi account Amazon SES.

Mettiamo tutti i nuovi account nella sandbox di Amazon SES. Lo stato della sandbox per il tuo account è unico per ogni account. Regione AWS Quando il tuo account è nella sandbox, puoi utilizzare tutte le caratteristiche di Amazon SES. Tuttavia, se il tuo account è nella sandbox, si applicano le seguenti limitazioni per il tuo account:

- Puoi inviare e-mail solo a indirizzi e-mail e domini verificati oppure al simulatore di mailbox Amazon SES.
- Puoi inviare un massimo di 200 messaggi per periodo di 24 ore.
- Puoi inviare un massimo di 1 messaggio al secondo.
- Per l'autorizzazione di invio, non è consentito inviare e-mail a indirizzi non verificati né all'utente, né al mittente delegato.
- Per la soppressione a livello di account, le azioni in blocco e le chiamate API SES relative alla gestione dell'elenco di soppressione sono disabilitate.

Quando il tuo account è uscito dalla sandbox e messo in produzione, puoi inviare e-mail a qualsiasi destinatario, indipendentemente dal fatto che l'indirizzo o il dominio del destinatario siano verificati. Tuttavia, devi comunque verificare ogni identità utilizzata come indirizzo "From" (Da), "Source" (Origine), "Sender" (Mittente) o "Return-Path" (Percorso di ritorno).

Completa le procedure in questa sezione per richiedere che il tuo account venga rimosso dalla sandbox e messo in produzione.

> **Note**
>
> - Se non hai ancora creato alcuna identità (indirizzo e-mail o dominio) in SES, puoi saltare le procedure in questa pagina e richiedere l'accesso di produzione per il tuo account utilizzando la procedura guidata di configurazione dell'account SES. Consulta Configurazione dell'account SES per istruzioni su come accedere alla procedura guidata.
> - Se utilizzi Amazon SES per inviare e-mail da un'istanza Amazon EC2, potrebbe anche essere necessario richiedere la rimozione della limitazione dalla porta 25 sull'istanza Amazon EC2. Per ulteriori informazioni, vedi Come faccio a rimuovere l'acceleratore sulla porta 25 dalla mia istanza EC2? nel Knowledge Center. AWS

Per richiedere l'accesso alla produzione (rimuovi l'account dalla sandbox) utilizzando il AWS Management Console

1. Aprire la console Amazon SES all'indirizzo https://console.aws.amazon.com/ses/.
2. Nel pannello di navigazione, scegli Dashboard dell'account.
3. Nella casella di avviso nella parte superiore della console con il messaggio "Your Amazon SES account is in the sandbox" (Il tuo account Amazon SES è nella sandbox), sul lato destro, scegli Request production access (Richiesta dell'accesso di produzione).
4. Nel modale dei dettagli dell'account, seleziona la casella di controllo Marketing o Transactional (Transazionali) che descrive al meglio la maggior parte dei messaggi che invierai.
   - E-mail di marketing: inviata su one-to-many base mirata a un elenco mirato di potenziali clienti o potenziali con contenuti di marketing e promozionali, ad esempio per effettuare acquisti, scaricare informazioni, ecc.
   - Email transazionale: inviata in modo univoco per ciascun destinatario, di solito attivata da un'azione dell'utente come un acquisto sul sito Web, una richiesta di reimpostazione della password, ecc. one-to-one
5. In Website URL (URL del sito Web), inserisci l'URL del tuo sito Web per aiutarci a capire meglio il tipo di contenuto che intendi inviare.
6. In Use case description (Descrizione del caso d'uso), spiega come intendi usare Amazon SES per inviare e-mail. Per aiutarci a elaborare la richiesta in modo più rapido, rispondi alle domande seguenti:
   - Come pensi di creare o acquisire l'elenco di indirizzi?

- Come pensi di gestire i mancati recapiti e i reclami?
- In che modo i destinatari possono scegliere di non ricevere le e-mail?
- Come hai scelto la frequenza di invio o la quota di invio specificate in questa richiesta?

7. In Additional contacts (Contatti aggiuntivi), comunicaci dove desideri ricevere comunicazioni relative al tuo account. Può trattarsi di un elenco di un massimo di 4 indirizzi e-mail, separati da virgole.
8. In Preferred contact language (Lingua di contatto preferita), scegli se le comunicazioni ricevute devono essere in English (Inglese) o Japanese (Giapponese).
9. In Acknowledgement (Conferma), seleziona la casella che accetti di inviare e-mail solo a persone che l'hanno esplicitamente richiesta e conferma di aver avviato un processo per la gestione delle notifiche di mancato recapito e reclamo.
10. Seleziona il pulsante Submit request (Inviare richiesta), verrà visualizzato un banner per confermare che la tua richiesta è stata inviata ed è attualmente in fase di revisione.

Dopo aver inviato una revisione dei dettagli del tuo account, non puoi modificarli fino al completamento della revisione. Il AWS Support team fornisce una prima risposta alla tua richiesta entro 24 ore.

Per evitare che i nostri sistemi vengano utilizzati per l'invio di contenuti indesiderati o dannosi, ogni richiesta dovrà essere analizzata attentamente da parte nostra. In seguito a questa valutazione, saremo in grado di gestire la tua richiesta durante le prime 24 ore. Tuttavia, se la risoluzione richiede l'invio di ulteriori informazioni da parte tua, i tempi di gestione della richiesta potranno essere più lunghi. Potremmo non essere in grado di gestire la tua richiesta se il caso d'uso specifico non è conforme con le nostre policy.

Facoltativamente, puoi anche inviare la tua richiesta di accesso alla produzione utilizzando il AWS CLI. L'invio della richiesta utilizzando il AWS CLI è utile quando desideri richiedere l'accesso alla produzione per un gran numero di identità o quando desideri automatizzare il processo di configurazione di Amazon SES.

Richiesta di rimozione dell'account dalla sandbox Amazon SES con AWS CLI

1. Prerequisito: devi prima installare e configurare l' AWS CLI. Per ulteriori informazioni, consulta la Guida per l'utente AWS Command Line Interface.
2. Nella riga di comando, inserisci il comando seguente:

```
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
```

Nel comando precedente, procedi come segue.

a. Sostituisci *TRANSACTIONAL* (TRANSAZIONALE) con il tipo di e-mail che intendi inviare tramite Amazon SES. È possibile specificare `TRANSACTIONAL` o `PROMOTIONAL`. Se si applicano più valori, specifica l'opzione adatta per la maggior parte delle e-mail che si intende inviare.

b. Sostituisci *https://example.com* con l'URL del tuo sito Web. Queste informazioni ci aiuteranno a comprendere meglio il tipo di contenuto che intendi inviare.

c. Sostituisci *Use case description* (Descrizione del caso d'uso) con una descrizione di come pensi di usare Amazon SES per inviare e-mail. Per aiutarci a elaborare la richiesta in modo più rapido, rispondi alle domande seguenti:

   i. Come pensi di creare o acquisire l'elenco di indirizzi?

   ii. Come pensi di gestire i mancati recapiti e i reclami?

   iii. In che modo i destinatari possono scegliere di non ricevere le e-mail?

   iv. Come hai scelto la frequenza di invio o la quota di invio specificate in questa richiesta?

d. Sostituisci *info@example.com* con gli indirizzi e-mail in cui desideri ricevere comunicazioni relative al tuo account. Può trattarsi di un elenco di un massimo di 4 indirizzi e-mail, separati da virgole.

e. Sostituisci *EN* con la lingua preferita. È possibile specificare `EN` per l'inglese o `JA` per il giapponese.

Dopo aver inviato una revisione dei dettagli del tuo account, non puoi modificarli fino al completamento della revisione. Il AWS Support team fornisce una prima risposta alla tua richiesta entro 24 ore.

Per evitare che i nostri sistemi vengano utilizzati per l'invio di contenuti indesiderati o dannosi, ogni richiesta dovrà essere analizzata attentamente da parte nostra. In seguito a questa valutazione,

saremo in grado di gestire la tua richiesta durante le prime 24 ore. Tuttavia, se la risoluzione richiede l'invio di ulteriori informazioni da parte tua, i tempi di gestione della richiesta potranno essere più lunghi. Potremmo non essere in grado di gestire la tua richiesta se il caso d'uso specifico non è conforme con le nostre policy.

Gestione dei limiti di invio di Amazon SES

Per ogni account Amazon SES è previsto un set di quote di invio per regolamentare il numero e la frequenza di messaggi e-mail che è possibile inviare. Le quote di invio avvantaggiano tutti i clienti Amazon SES perché aiutano a mantenere la relazione attendibile tra Amazon SES e i provider di posta elettronica. Le quote di invio sono utili per incrementare gradualmente le attività di invio e diminuire la probabilità che i provider di posta elettronica blocchino le e-mail a causa di picchi improvvisi non previsti nel volume o nella frequenza di invio delle e-mail.

Le seguenti quote si applicano all'invio di e-mail tramite Amazon SES:

- Quota di invio: il numero massimo di e-mail che è possibile inviare in un periodo di tempo di 24 ore. Tale quota è calcolata su un periodo di tempo continuo. Ogni volta che tenti di inviare un'e-mail, Amazon SES determina il numero di e-mail che hai inviato nelle 24 ore precedenti. Finché il numero totale di e-mail che hai inviato nelle ultime 24 ore è inferiore a questo massimo giornaliero, la tua richiesta di invio viene accettata e la tua e-mail viene inviata.

  Se l'invio di un messaggio supera il massimo giornaliero per il tuo account, la chiamata ad Amazon SES viene rifiutata.
- Frequenza massima in uscita: il numero massimo di e-mail al secondo che Amazon SES può accettare dal tuo account. Puoi superare questa quota per brevi picchi, ma non per un lungo periodo di tempo.

  > **Note**
  >
  > La velocità con cui Amazon SES accetta i tuoi messaggi può essere inferiore alla frequenza massima in uscita per il tuo account.

- Dimensione massima del messaggio (MB): la dimensione massima dell'e-mail che puoi inviare. Ciò include tutte le immagini e gli allegati che fanno parte dell'e-mail dopo la codifica MIME. Ad esempio, se alleghi un file di 5 MB, la dimensione dell'allegato nell'e-mail dopo la codifica MIME sarà di circa 6,85 MB (circa il 137% delle dimensioni del file originale).

  > **Note**
  >
  > Ti consigliamo di caricare gli allegati sulle unità cloud e di includere l'URL dell'allegato dell'unità cloud per ridurre le dimensioni delle e-mail e migliorare la capacità di recapitare i messaggi. SES non può garantire che i messaggi di posta elettronica di grandi dimensioni

finiscano nella cassetta postale del destinatario in quanto diversi server di posta avranno criteri basati su dimensioni variabili.

Le quote di invio Amazon SES sono separate per ogni Regione AWS. Per informazioni sull'uso di Amazon SES in più regioni AWS, consulta Regioni e Amazon SES.

Quando il tuo account si trova nella sandbox di Amazon SES, la tua quota di invio è di 200 messaggi per un periodo di 24 ore e la frequenza massima di invio è di un messaggio al secondo. Quando invii una richiesta di rimozione del tuo account dalla sandbox, puoi anche contemporaneamente richiedere che le tue quote vengano aumentate. Per informazioni su come ottenere la rimozione dell'account dalla sandbox, consulta Richiedi l'accesso alla produzione (uscita dalla sandbox di Amazon SES).

Quando l'account è stato rimosso dalla sandbox, è possibile richiedere ulteriori aumenti delle quote in qualsiasi momento creando una nuova pratica nel Centro assistenza AWS. Per ulteriori informazioni, consultare Aumento delle quote di invio di Amazon SES.

> **Note**
>
> Le quote di invio si basano sui destinatari e non sui messaggi. Ad esempio, un'e-mail con 10 destinatari viene conteggiata come 10 e-mail ai fini della quota. Tuttavia, si sconsiglia di inviare un messaggio e-mail a più destinatari in una singola chiamata all'operazione API `SendEmail`, poiché se la chiamata non riesce, l'intera e-mail viene respinta. È consigliabile effettuare la chiamata a `SendEmail` una volta per ogni destinatario.

- Per aumentare le quote di invio, consulta Aumento delle quote di invio di Amazon SES.
- Per monitorare le quote di invio utilizzando la console Amazon SES o l'API Amazon SES, consulta Monitoraggio delle quote di invio di Amazon SES.
- Per ulteriori informazioni sugli errori che la tua applicazione riceve quando raggiungi le quote di invio, consulta Errori relativi alle quote di invio per l'account Amazon SES.

Aumento delle quote di invio di Amazon SES

Di seguito sono riportate le quote dell'account in relazione alla Regione corrente che possono essere aumentate.

Risorsa	Quota predefinita	Descrizione
Quota di invio	200	Il numero massimo di e-mail che è possibile inviare in un periodo di tempo di 24 ore nell'attuale Regione AWS.
Frequenza di invio	1	Il numero massimo di e-mail che Amazon SES può accettare ogni secondo per questo account nell'attuale Regione AWS.

Aumento automatico delle quote di invio

Quando il tuo account è esterno alla sandbox e stai inviando e-mail di produzione di alta qualità, potremmo aumentare automaticamente le quote di invio per il tuo account. Spesso, aumentiamo automaticamente queste quote prima che tu ne abbia effettivamente bisogno.

Per qualificarsi per gli aumenti automatici della velocità, tutte le seguenti affermazioni devono essere vere:

- Invii contenuti di alta qualità che i tuoi destinatari desiderano ricevere: invii contenuti che i destinatari desiderano e aspettano. Smetti di inviare e-mail ai clienti che non le aprono.
- Invii contenuto di produzione effettivo: l'invio di messaggi di prova a indirizzi e-mail falsi può avere un impatto negativo sulle percentuali di mancati recapiti e reclami. Inoltre, l'invio di messaggi solo a destinatari interni rende difficile determinare se stai inviando contenuti che i clienti desiderano ricevere. Tuttavia, quando invii i tuoi messaggi di produzione a destinatari non interni, possiamo valutare con precisione le tue procedure di invio di e-mail.
- Invii avvicinandoti alla quota corrente: per qualificarti per un aumento automatico del limite, il tuo volume giornaliero di e-mail deve avvicinarsi regolarmente alla tua quota senza superarla.
- La percentuale di mancati recapiti e reclami è bassa: riduci al minimo il numero di mancati recapiti e reclami che ricevi. Un numero elevato di mancati recapiti e reclami può avere un impatto negativo sulle quote di invio.

L'utente ha richiesto maggiori quote di invio

Se le attuali quote di invio non sono adeguate alle proprie esigenze e non sono state automaticamente aumentate, è possibile richiedere un aumento:

- Quota di invio o Frequenza di invio: le relative richieste di aumento possono essere inviate tramite la console AWS Service Quotas.

Richiesta di un aumento delle quote di invio Amazon SES tramite la console Service Quotas.

1. Apri la console Service Quotas.
2. Seleziona la Regione per la quale desideri aumentare utilizzando il menu a discesa nell'angolo in alto a destra della console (accanto al tuo numero di account).
3. Nel pannello di navigazione, scegli AWS services (Servizi AWS).
4. Scegli Amazon Simple Email Service (SES).
5. Scegli una quota e segui le istruzioni per richiedere un aumento di quota.

> **SLA del team AWS Support per i tipi di richieste di aumento**
>
> Per evitare che i nostri sistemi vengano utilizzati per l'invio di contenuti indesiderati o dannosi, ogni richiesta dovrà essere analizzata attentamente da parte nostra. In seguito a questa verifica, saremo in grado di garantire la tua richiesta nei tempi specificati indicati di seguito per il tipo di aumento richiesto. Tuttavia, se la risoluzione richiede l'invio di ulteriori informazioni da parte tua, i tempi di gestione della richiesta potranno essere più lunghi. Ci riserviamo il diritto di non garantire la tua richiesta se il tuo caso d'uso non è conforme con le nostre policy.
>
> - Sending quota or Sending rate (Quota di invio o Frequenza di invio): fino a 24 ore.

> **Note**
>
> Sebbene la console Service Quotas sia disponibile in molte lingue diverse, il supporto effettivo è fornito solo in inglese.

Monitoraggio delle quote di invio di Amazon SES

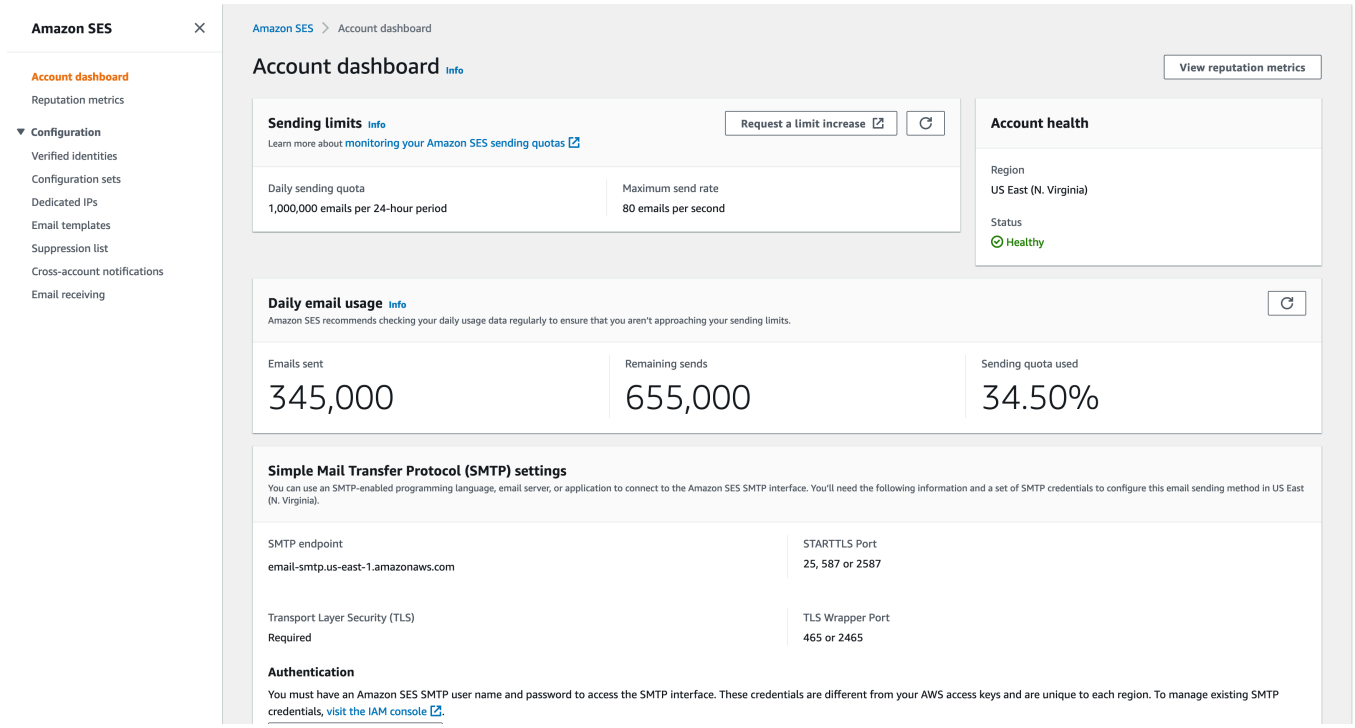
Puoi monitorare le quote di invio utilizzando la console o mediante l'API Amazon SES, chiamando l'interfaccia di query (HTTPS) direttamente o indirettamente, tramite SDK AWS, AWS Command Line Interface o AWS Tools for Windows PowerShell.

> **Important**
>
> Consigliamo di controllare spesso le statistiche di invio per essere certi di non essere prossimi al raggiungimento delle quote di invio. Se hai quasi raggiunto le quote di invio, consulta Aumento delle quote di invio di Amazon SES per informazioni su come aumentarle. Non aspettare di raggiungere le quote di invio per aumentarle.

Monitoraggio delle quote di invio mediante la console Amazon SES

La procedura seguente mostra come visualizzare le quote di invio tramite la console Amazon SES.

1. Accedere alla AWS Management Console e aprire la console Amazon SES all'indirizzo https://console.aws.amazon.com/ses/.
2. Nel pannello di navigazione, scegli Account dashboard (Pannello di controllo account). Le quote di invio sono indicate in Sending Limits (Limiti di invio). Le e-mail totali inviate, i restanti invii e la percentuale di quota di invio utilizzata vengono visualizzati in Daily email usage (Utilizzo giornaliero delle e-mail).



3. Per aggiornare la visualizzazione, seleziona l'icona di aggiornamento nell'angolo in alto a destra della casella Daily email usage (Utilizzo giornaliero delle e-mail).

Monitoraggio delle quote di invio mediante l'API Amazon SES

L'API Amazon SES dispone dell'operazione `GetSendQuota`, che restituisce le quote di invio. Quando chiami l'operazione `GetSendQuota`, ricevi le informazioni seguenti:

- numero di e-mail che hai inviato nelle ultime 24 ore;
- quota di invio per il periodo corrente di 24 ore;
- frequenza massima in uscita.

> **Note**
>
> Per una descrizione completa di `GetSendQuota`, vai alla pagina Documentazione di riferimento delle API Amazon Simple Email Service.

Errori relativi alle quote di invio per l'account Amazon SES

Se tenti di inviare un'e-mail dopo aver raggiunto la quota di invio giornaliera (il numero massimo di e-mail che puoi inviare in un periodo di 24 ore) o la frequenza massima in uscita (il numero massimo di messaggi che puoi inviare al secondo), Amazon SES ignorerà il messaggio e non tenterà di inviarlo nuovamente. Amazon SES fornisce inoltre un messaggio di errore che spiega il problema. Amazon SES fornisce anche un messaggio di errore che spiega il problema. Il modo in cui Amazon SES produce tale messaggio di errore dipende dal modo in cui hai tentato di inviare l'e-mail. Questo argomento include informazioni sui messaggi ricevute tramite l'API Amazon SES e attraverso un'interfaccia SMTP.

Per indicazioni su una tecnica che puoi utilizzare quando raggiungi la frequenza massima in uscita, consulta come gestire un errore di superamento della frequenza massima in uscita con conseguente limitazione nel blog targeting e messaggistica AWS.

Raggiungimento dei limiti di invio con l'API Amazon SES

Se tenti di inviare un'e-mail utilizzando l'API Amazon SES (o un SDK AWS), ma hai già superato i limiti di invio dell'account, l'API genera un errore `ThrottlingException`. Il messaggio di errore include uno dei seguenti messaggi:

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

Se riscontri un errore di limitazione, dovresti programmare l'applicazione in modo che attenda un intervallo di tempo fino a 10 minuti prima di ripetere l'invio della richiesta.

Raggiungimento dei limiti di invio con SMTP

Se tenti di inviare un'e-mail utilizzando l'interfaccia SMTP Amazon SES, ma hai già superato i limiti di invio dell'account, il client SMTP potrebbe visualizzare uno dei seguenti errori:

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

Client SMTP differenti gestiscono questi errori in diversi modi.

Configurazione dell'invio di e-mail con Amazon SES

È possibile inviare un messaggio e-mail con Amazon Simple Email Service (Amazon SES) utilizzando la console Amazon SES, l'interfaccia SMTP (Simple Mail Transfer Protocol) Amazon SES o l'API Amazon SES. In genere si usa la console per l'invio di e-mail di test e la gestione dell'attività di invio. Per inviare e-mail in blocco, è possibile usare l'interfaccia SMTP o l'API. Per informazioni sui prezzi per e-mail in Amazon SES, consulta la pagina Prezzi di Amazon SES.

- Se desideri usare un linguaggio di programmazione, un'applicazione o un pacchetto software compatibile con SMTP per l'invio di e-mail tramite Amazon SES oppure integrare Amazon SES con il server di posta esistente, usa l'interfaccia SMTP Amazon SES. Per ulteriori informazioni, consulta Invio di e-mail a livello di programmazione tramite l'interfaccia SMTP di Amazon SES.
- Se desideri chiamare Amazon SES usando richieste HTTP non elaborate, usa l'API Amazon SES. Per ulteriori informazioni, consulta Utilizzo dell'API Amazon SES per l'invio di e-mail.

> **Important**
>
> Quando invii un'e-mail a più destinatari (ossia gli indirizzi specificati nelle caselle "A", "Cc" e "Ccn") e la chiamata ad Amazon SES ha esito negativo, l'intera e-mail viene respinta e nessuno dei destinatari la riceve. Consigliamo quindi di inviare un'e-mail a un destinatario per volta.

Utilizzo dell'interfaccia SMTP Amazon SES per inviare e-mail

Per inviare e-mail di produzione tramite Amazon SES, puoi utilizzare l'interfaccia Simple Mail Transfer Protocol (SMTP) o l'API Amazon SES. Per ulteriori informazioni sull'API Amazon SES, consulta Utilizzo dell'API Amazon SES per l'invio di e-mail. Questa sezione descrive l'interfaccia SMTP.

Amazon SES invia e-mail tramite SMTP, ovvero il protocollo e-mail più comune su Internet. Puoi inviare e-mail tramite Amazon SES utilizzando un'ampia gamma di linguaggi di programmazione e programmi software compatibili con SMTP per connetterti all'interfaccia SMTP Amazon SES. Questa sezione spiega come ottenere le credenziali SMTP Amazon SES, come inviare e-mail utilizzando l'interfaccia SMTP e come configurare più programmi software e server di posta per l'utilizzo di Amazon SES per l'invio di e-mail.

Per le soluzioni a problemi comuni che possono verificarsi quando utilizzi Amazon SES tramite l'interfaccia SMTP, consulta Problemi relativi a SMTP in Amazon SES.

Requisiti per l'invio di e-mail tramite SMTP

Per inviare e-mail utilizzando l'interfaccia SMTP Amazon SES, è necessario quanto segue:

- L'indirizzo dell'endpoint SMTP. Per un elenco degli endpoint SMTP Amazon SES, consulta Connessione a un endpoint SMTP Amazon SES.
- Il numero di porta dell'interfaccia SMTP. Il numero di porta varia in base al metodo di connessione. Per ulteriori informazioni, consulta Connessione a un endpoint SMTP Amazon SES.
- Nome utente e password SMTP. Le credenziali SMTP sono univoche per ogni regione AWS . Se pensi di utilizzare l'interfaccia SMTP per inviare e-mail in più regioni AWS , hai bisogno di credenziali SMTP per ogni regione.

> **Important**
>
> Le tue credenziali SMTP non sono identiche alle tue chiavi di AWS accesso o alle credenziali che usi per accedere alla console Amazon SES. Per informazioni su come generare le credenziali SMTP, consulta Richiesta delle credenziali SMTP Amazon SES.

- Un software client che possa comunicare utilizzando Transport Layer Security (TLS). Per ulteriori informazioni, consulta Connessione a un endpoint SMTP Amazon SES.
- Un indirizzo e-mail verificato con Amazon SES. Per ulteriori informazioni, consulta Identità verificate in Amazon SES.
- Incremento delle quote di invio, se desideri inviare grandi quantità di e-mail. Per ulteriori informazioni, consulta Gestione dei limiti di invio di Amazon SES.

Metodi per inviare e-mail tramite SMTP

È possibile inviare e-mail tramite SMTP tramite uno dei seguenti metodi:

- Per configurare un prodotto software compatibile con SMTP per l'invio di e-mail tramite l'interfaccia SMTP Amazon SES, consulta Invio di e-mail tramite Amazon SES mediante pacchetti software.
- Per programmare un'applicazione per l'invio di e-mail tramite Amazon SES, consulta Invio di e-mail a livello di programmazione tramite l'interfaccia SMTP di Amazon SES.

- Per configurare il server di posta esistente per l'invio di tutti i messaggi in uscita tramite Amazon SES, consulta Integrazione di Amazon SES con il server e-mail esistente.
- Per interagire con l'interfaccia SMTP Amazon SES tramite la riga di comando, utile per le attività di test, consulta Verifica della connessione all'interfaccia SMTP Amazon SES utilizzando la riga di comando.

Per un elenco di codici di risposta SMTP, consulta Codici di risposta SMTP restituiti da Amazon SES.

Informazioni da fornire per le e-mail

Quando accedi ad Amazon SES attraverso l'interfaccia SMTP, l'applicazione client SMTP assembla il messaggio, perciò le informazioni che devi fornire dipendono dall'applicazione in uso. Come minimo, lo scambio SMTP tra un client e un server richiede quanto segue:

- un indirizzo IP di origine;
- un indirizzo di destinazione;
- dati del messaggio

Se utilizzi l'interfaccia SMTP e hai abilitato l'inoltro del feedback, le notifiche di mancato recapito (bounce), reclamo e consegna vengono inviate all'indirizzo "MAIL FROM". Qualsiasi indirizzo "Reply-To" specificato non viene utilizzato.

Richiesta delle credenziali SMTP Amazon SES

Sono necessarie credenziali SMTP di Amazon SES per accedere all'interfaccia SMTP di SES.

Le credenziali che usi per inviare e-mail tramite l'interfaccia SMTP di SES sono uniche per ogni regione. AWS Se utilizzi l'interfaccia SMTP di SES per l'invio di e-mail in più di una Regione, è necessario generare un set di credenziali SMTP per ogni Regione che prevedi di utilizzare.

La password SMTP è diversa dalla chiave di accesso AWS segreta. Per ulteriori informazioni sulle credenziali, consulta Tipi di credenziali Amazon SES.

> **Note**
>
> Gli endpoint SMTP non sono attualmente disponibili in Africa (Città del Capo), Asia Pacifico (Giacarta), Europa (Milano), Israele (Tel Aviv) e Medio Oriente (Bahrain).

Ottenimento delle credenziali SMTP SES mediante la console SES

Quando usi il flusso di lavoro SES sottostante per generare credenziali SMTP utilizzando la console, viene visualizzata la console IAM per creare un utente con le policy appropriate per chiamare SES e che fornisce le credenziali SMTP associate a tale utente.

Requisito

Un utente IAM può creare credenziali SMTP SES, ma la policy dell'utente deve concedere all'utente stesso l'autorizzazione a utilizzare IAM, perché le credenziali SMTP SES vengono create tramite IAM. La tua policy IAM deve consentire di eseguire le seguenti operazioni IAM: `iam:ListUsers`, `iam:CreateUser`, `iam:CreateAccessKey` e `iam:PutUserPolicy`. Se provi a creare credenziali SMTP SES utilizzando la console e il tuo utente IAM non dispone di queste autorizzazioni, visualizzerai un errore che indica che il tuo account «non è autorizzato a eseguire iam:». ListUsers

Creazione delle credenziali SMTP

1. Accedi AWS Management Console e apri la console Amazon SES all'indirizzo https://console.aws.amazon.com/ses/.
2. Scegliere SMTP settings (Impostazioni SMTP) nel riquadro di navigazione sinistro; verrà visualizzata la pagina Simple Mail Transfer Protocol (SMTP) settings (Impostazioni SMTP (Simple Mail Transfer Protocol).
3. Scegliere Create SMTP Credentials (Crea credenziali SMTP) nell'angolo superiore destro: si aprirà la console IAM.
4. (Facoltativo) Se è necessario visualizzare, modificare o eliminare gli utenti SMTP che già creati, scegliere Manage my existing SMTP credentials (Gestisci le mie credenziali SMTP esistenti) nell'angolo inferiore destro: si aprirà la console IAM. I dettagli per la gestione delle credenziali SMTP vengono forniti seguendo queste procedure.
5. In Crea utente per SMTP, digita un nome per l'utente SMTP nel campo Nome utente IAM. In alternativa, puoi utilizzare il valore predefinito che viene fornito in questo campo. Al termine, scegli Crea nell'angolo in basso a destra.
6. Seleziona Mostra sotto Password SMTP: le tue credenziali SMTP vengono visualizzate sullo schermo.
7. Scarica queste credenziali scegliendo Scarica credenziali o copiale e archiviale in un luogo sicuro, poiché non puoi visualizzarle o salvarle dopo aver chiuso questa finestra di dialogo.
8. Scegli Torna alla console SES.

È possibile visualizzare l'elenco delle credenziali SMTP create con questa procedura nella console IAM in Access management (Gestione degli accessi) e scegliendo Users (Utenti) seguito dall'utilizzo della barra di ricerca per trovare tutti gli utenti a cui sono state assegnate le credenziali SMTP.

Puoi anche utilizzare la console IAM per eliminare gli utenti SMTP esistenti. Per ulteriori informazioni sull'eliminazione degli utenti, consulta Gestione degli utenti IAM nella Guida alle operazioni di base di IAM.

Per modificare la password SMTP, elimina l'utente SMTP esistente nella console IAM. Quindi, completa le procedure precedenti per generare un nuovo set di credenziali SMTP.

Ottenere le credenziali SMTP SES convertendo le credenziali esistenti AWS

Se hai un utente configurato utilizzando l'interfaccia IAM, puoi ricavare le credenziali SMTP SES dell'utente dalle sue credenziali. AWS

> **Important**
>
> Non utilizzare AWS credenziali temporanee per derivare credenziali SMTP. L'interfaccia SMTP SES non supporta credenziali SMTP generate da credenziali di sicurezza temporanee.

Per abilitare l'utente IAM all'invio di e-mail utilizzando l'interfaccia SMTP SES, procedi come segue.

- Ricava le credenziali SMTP dell'utente dalle relative credenziali utilizzando l'algoritmo AWS fornito in questa sezione. Poiché si parte dalle AWS credenziali, il nome utente SMTP è lo stesso dell'ID della chiave di AWS accesso, quindi è sufficiente generare la password SMTP.
- Applica la policy seguente all'utente IAM:

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

Per ulteriori informazioni sull'uso di SES con IAM, consulta Identity and Access Management in Amazon SES.

> **Note**
>
> Anche se puoi generare le credenziali SMTP SES per qualsiasi utente IAM, ti consigliamo di creare un utente IAM distinto quando generi le credenziali SMTP. Per ulteriori informazioni sui motivi per cui è consigliabile creare utenti per scopi specifici, consulta Best practice IAM.

Il seguente pseudocodice mostra l'algoritmo che converte una chiave di accesso AWS segreta in una password SMTP SES.

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

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

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

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

Alcuni linguaggi di programmazione comprendono librerie che puoi utilizzare per convertire una chiave di accesso segreta IAM in una password SMTP. Questa sezione include un esempio di codice che è possibile utilizzare per convertire una chiave di accesso AWS segreta in una password SMTP SES utilizzando Python.

> **Note**
>
> Il seguente esempio usa stringhe f introdotte in Python 3.6; con una versione precedente non funzioneranno.
> Attualmente, l'SDK di Python (Boto3) supporta ufficialmente 2.7 e 3.6 (o versioni successive). Tuttavia, il supporto per la versione 2.7 è obsoleto e verrà eliminato il 15/7/2021, quindi sarà necessario eseguire l'aggiornamento almeno alla versione 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()
```

Per ottenere la password SMTP utilizzando questo script, salva il codice precedente come `smtp_credentials_generate.py`. Quindi, nella riga di comando eseguire il comando riportato di seguito:

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

Nel comando precedente, procedi come segue.

- Sostituisci *path/to/* con il percorso in cui hai salvato `smtp_credentials_generate.py`.
- Sostituisci *WJALRXUTNFemi/K7MDEng/b PxRfi CYEXAMPLEKEY con la chiave di accesso segreta* che desideri convertire in una password SMTP.
- Sostituisci *us-east-1* con AWS la regione in cui desideri utilizzare le credenziali SMTP.

Quando questo script viene eseguito correttamente, l'unico output è la password SMTP.

Connessione a un endpoint SMTP Amazon SES

Per inviare e-mail utilizzando l'interfaccia SMTP Amazon SES, è necessario connettere l'applicazione a un endpoint SMTP. Per un elenco completo degli endpoint SMTP Amazon SES, consulta Endpoint e quote di Amazon Simple Email Service in Riferimenti generali di AWS.

L'endpoint SMTP Amazon SES richiede che tutte le connessioni siano crittografate tramite Transport Layer Security (TLS). TLS è spesso indicato con il nome del suo predecessore, il protocollo SSL (Secure Sockets Layer). Amazon SES supporta due meccanismi per stabilire una connessione crittografata tramite TLS: STARTTLS e TLS Wrapper. Consulta la documentazione del software per determinare se supporta STARTTLS, TLS Wrapper o entrambi.

Amazon Elastic Compute Cloud (Amazon EC2) limita il traffico e-mail sulla porta 25 per impostazione predefinita. Per evitare timeout durante l'invio di e-mail tramite l'endpoint SMTP da EC2, invia una richiesta di rimozione dei limiti di invio di e-mail per rimuovere la limitazione. In alternativa, è possibile inviare e-mail utilizzando una porta diversa o tramite un Endpoint Amazon VPC.

Per problemi di connessione SMTP, consulta Problemi relativi a SMTP.

STARTTLS

STARTTLS permette di aggiornare una connessione non crittografata in connessione crittografata. Esistono versioni di STARTTLS per diversi protocolli; la versione SMTP è definita nello standard RFC 3207.

Per impostare una connessione STARTTLS, il client SMTP si connette all'endpoint SMTP Amazon SES sulla porta 25, 587 o 2587, invia un comando EHLO e attende che il server annunci di supportare l'estensione SMTP STARTTLS. Il client invia quindi il comando STARTTLS, avviando la negoziazione TLS. Al termine della negoziazione, il client invia un comando EHLO tramite la nuova connessione crittografata e la sessione SMTP procede normalmente.

TLS Wrapper

TLS Wrapper, noto anche come SMTPS o protocollo Handshake, permette di avviare una connessione crittografata senza prima stabilire una connessione non crittografata. Con TLS Wrapper l'endpoint SMTP Amazon SES non esegue la negoziazione TLS, ma è responsabilità del client connettersi all'endpoint tramite TLS e continuare a usare TLS per l'intera conversazione. TLS Wrapper è un protocollo meno recente, ma è supportato da molti client.

Per configurare una connessione TLS Wrapper, il client SMTP si connette all'endpoint SMTP Amazon SES sulla porta 465 o 2465. Il server presenta il proprio certificato, il client invia un comando EHLO e la sessione SMTP procede normalmente.

Invio di e-mail tramite Amazon SES mediante pacchetti software

Sono disponibili diversi pacchetti software commerciali e open source che supportano l'invio di e-mail tramite il protocollo SMTP. Ecco alcuni esempi:

- Piattaforme per blog
- Aggregatori RSS
- Software di gestione elenchi
- Sistemi di gestione dei flussi di lavoro

Puoi configurare qualsiasi prodotto software compatibile con SMTP di questo tipo per l'invio di e-mail tramite l'interfaccia SMTP Amazon SES. Per istruzioni su come configurare il protocollo SMTP per un determinato pacchetto software, consulta la documentazione del software.

La procedura seguente mostra come configurare l'invio tramite Amazon SES in JIRA, una diffusa soluzione di gestione dei problemi. Con questa configurazione, JIRA è in grado di inviare notifiche via e-mail agli utenti se si verificano modifiche nello stato di un problema software.

Configurazione di JIRA per l'invio di e-mail tramite Amazon SES

1. Utilizzando il browser Web, accedi a JIRA con le credenziali di amministratore.

2. Nella finestra del browser scegli Administration (Amministrazione).
3. Nel menu System (Sistema) scegli Mail (Posta).
4. Nella pagina Mail administration (Amministrazione posta) scegli Mail Servers (Server di posta).
5. Scegli Configure new SMTP mail server (Configura nuovo server di posta SMTP).
6. Nel modulo Add SMTP Mail Server (Aggiungi server di posta SMTP) compila i campi seguenti:

   a. Name (Nome): un nome descrittivo per questo server.

   b. From address (Indirizzo mittente): l'indirizzo da cui verranno inviate le e-mail. Dovrai verificare questo indirizzo e-mail con Amazon SES prima di poterlo usare. Per ulteriori informazioni sulla verifica, consulta Identità verificate in Amazon SES.

   c. Email prefix (Prefisso e-mail): una stringa che JIRA antepone a ogni oggetto prima dell'invio.

   d. Protocol (Protocollo): scegli SMTP.

   > **Note**
   >
   > Se non riesci a connetterti ad Amazon SES utilizzando questa impostazione, prova SECURE_SMTP.

   e. Hostname (Nome host): consulta Connessione a un endpoint SMTP Amazon SES per un elenco di endpoint SMTP Amazon SES. Ad esempio, se desideri utilizzare l'endpoint Amazon SES nella Regione Stati Uniti occidentali (Oregon), il nome host sarà email-smtp.us-west-2.amazonaws.com.

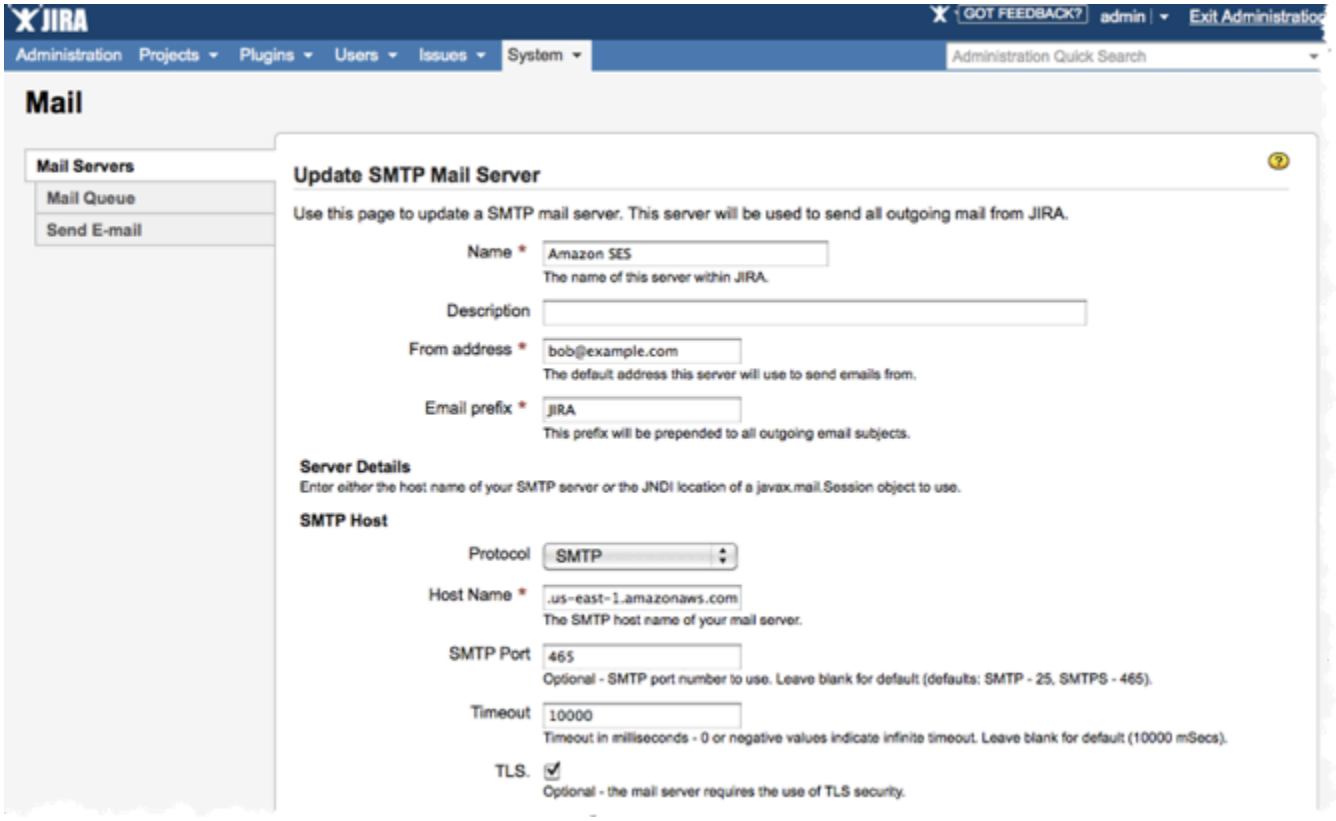
   f. SMTP Port (Porta SMTP): 25, 587 o 2587 (per la connessione con STARTTLS) oppure 465 o 2465 (per la connessione con TLS Wrapper).

   g. TLS: seleziona questa casella di controllo.

   h. User name (Nome utente): il tuo nome utente SMTP.

   i. Password: la tua password SMTP.

   È possibile visualizzare le impostazioni per TLS Wrapper nella seguente immagine.



7. Scegli Test Connection (Connessione di prova). Se l'e-mail di prova che JIRA invia tramite Amazon SES arriva correttamente, la configurazione è completa.

Invio di e-mail a livello di programmazione tramite l'interfaccia SMTP di Amazon SES

Per inviare un'e-mail utilizzando l'interfaccia SMTP di Amazon SES, puoi utilizzare linguaggi di programmazione, server e-mail o applicazione compatibili con SMTP. Prima di iniziare, completa le attività in Impostazione di Amazon Simple Email Service. È inoltre necessario disporre delle seguenti informazioni aggiuntive:

- Il nome utente e la password SMTP di SES, che ti permettono di connetterti all'endpoint SMTP di Amazon SES. Per ottenere le credenziali SMTP Amazon SES, consulta Richiesta delle credenziali SMTP Amazon SES.

> **Important**
>
> Le tue credenziali SMTP sono diverse dalle tue credenziali. AWS Per ulteriori informazioni sulle credenziali, consulta Tipi di credenziali Amazon SES.

- L'indirizzo dell'endpoint SMTP. Per un elenco degli endpoint SMTP Amazon SES, consulta Connessione a un endpoint SMTP Amazon SES.
- Il numero di porta dell'interfaccia SMTP di Amazon SES, il quale dipende dal metodo di connessione. Per ulteriori informazioni, consulta Connessione a un endpoint SMTP Amazon SES.

Integrazione di Amazon SES con il server e-mail esistente

Se amministri il tuo server e-mail, puoi utilizzare l'endpoint SMTP Amazon SES per inviare tutte le e-mail in uscita verso Amazon SES. Non è necessario modificare i client e le applicazioni e-mail esistenti; il passaggio ad Amazon SES sarà trasparente.

Diversi server di posta elettronica (MTA) supportano l'invio di e-mail tramite inoltro SMTP. Questa sezione fornisce indicazioni generali su come configurare alcuni dei più diffusi MTA per l'invio di e-mail tramite l'interfaccia SMTP Amazon SES.

L'endpoint SMTP Amazon SES richiede che tutte le connessioni siano crittografate tramite Transport Layer Security (TLS).

Argomenti

- Integrazione di Amazon SES con il server SMTP IIS di Microsoft Windows Server

Integrazione di Amazon SES con il server SMTP IIS di Microsoft Windows Server

Puoi configurare il server SMTP IIS di Microsoft Windows Server per l'invio di e-mail tramite Amazon SES. Queste istruzioni si riferiscono a Microsoft Windows Server 2012 su un'istanza Amazon EC2. Puoi utilizzare la stessa configurazione su Microsoft Windows Server 2008 e Microsoft Windows Server 2008 R2.

> **Note**
>
> Windows Server è un'applicazione di terze parti e non è sviluppata o supportata da Amazon Web Services. Le procedure descritte in questa sezione sono fornite solo a scopo informativo e sono soggette a modifiche senza preavviso.

Integrazione del server SMTP IIS di Microsoft Windows Server con Amazon SES

1. In primo luogo, configura Microsoft Windows Server 2012 utilizzando le seguenti istruzioni.
   a. Dalla console di gestione Amazon EC2; avvia una nuova istanza Amazon EC2 base di Microsoft Windows Server 2012.
   b. Connettiti all'istanza ed esegui l'accesso utilizzando Desktop remoto, seguendo le istruzioni in Nozioni di base sulle istanze Windows di Amazon EC2.
   c. Avvia il pannello di controllo Server Manager.
   d. Installa il ruolo Web Server (Server Web). Assicurati di includere IIS 6 Management Compatibility tools (strumenti di compatibilità di gestione IIS 6), un'opzione sotto la casella di controllo Web Server (Server Web).
   e. Installa la funzionalità SMTP Server (Server SMTP).
2. Quindi, configura il servizio SMTP IIS utilizzando le seguenti istruzioni.
   a. Torna al pannello di controllo Server Manager.
   b. Nel menu Tools (Strumenti), scegli Internet Information Services (IIS) 6.0 Manager.
   c. Fai clic con il pulsante destro del mouse su SMTP Virtual Server #1 (Server virtuale SMTP n. 1), quindi seleziona Properties (Proprietà).
   d. Nella scheda Access (Accesso), in Relay Restrictions (Restrizioni di inoltro), scegli Relay (Inoltro).
   e. Nella finestra di dialogo Relay Restrictions (Restrizioni di inoltro), scegli Add (Aggiungi).
   f. In Single Computer (Computer singolo), immetti 127.0.0.1 per l'indirizzo IP. Con queste operazioni hai concesso l'accesso a questo server per l'inoltro delle e-mail ad Amazon SES tramite il servizio SMTP IIS.

      In questa procedura, presupponiamo che le tue e-mail vengono generate su questo server. Se l'applicazione che genera le e-mail viene eseguita su un altro server, devi concedere l'accesso di inoltro a quel server in SMTP IIS.

> **Note**
>
> Per estendere l'inoltro SMTP a sottoreti private, per Relay Restriction (Restrizioni di inoltro) utilizza Single Computer (Computer singolo) 127.0.0.1 e Group of Computers (Gruppo di computer) 172.1.1.0 - 255.255.255.0 (nella sezione netmask (Maschera di rete)). Per Connection (Connessione), utilizza Single Computer (Computer singolo) 127.0.0.1 e Group of Computers (Gruppo di computer) 172.1.1.0 - 255.255.255.0 (nella sezione netmask (Maschera di rete)).

3. Infine, configura il server per l'invio di e-mail tramite Amazon SES utilizzando le istruzioni seguenti.

   a. Torna alla finestra di dialogo SMTP Virtual Server #1 Properties (Proprietà del server virtuale SMTP n. 1), quindi scegli la scheda Delivery (Recapito).

   b. Nella scheda Delivery (Recapito), scegli Outbound Security (Protezione connessioni in uscita).

   c. Seleziona Basic Authentication (Autenticazione di base), quindi immetti le credenziali SMTP SES. Puoi ottenere tali credenziali dalla console Amazon SES utilizzando la procedura descritta in Richiesta delle credenziali SMTP Amazon SES.

   > **Important**
   >
   > Le credenziali SMTP non sono le stesse dell'ID della chiave di accesso e della chiave di AWS accesso segreta. Non tentate di utilizzare AWS le vostre credenziali per autenticarvi sull'endpoint SMTP. Per ulteriori informazioni sulle credenziali, consulta Tipi di credenziali Amazon SES.

   d. Verifica che la voce TLS encryption (Crittografia TLS) sia selezionata.

   e. Torna alla scheda Delivery (Recapito).

   f. Scegli Outbound Connections (Connessioni in uscita).

   g. Nella finestra di dialogo Outbound Connections (Connessioni in uscita), verifica che la porta sia 25 o 587.

   h. Scegli Advanced (Avanzato).

   i. Per Smart host, immetti l'endpoint Amazon SES che utilizzerai (ad esempio, email-smtp.us-west-2.amazonaws.com). Per un elenco degli URL degli endpoint per i Regioni AWS quali

è disponibile Amazon SES, consulta Amazon Simple Email Service (Amazon SES) nel. Riferimenti generali di AWS

j. Torna al pannello di controllo Server Manager.

k. Nel pannello di controllo Server Manager fai clic con il pulsante destro del mouse su SMTP Virtual Server #1 (Server virtuale SMTP n. 1), quindi riavvia il servizio per attivare la nuova configurazione.

l. Invia un'e-mail tramite questo server. Puoi esaminare le intestazioni del messaggio per verificare che è stato recapitato tramite Amazon SES.

Verifica della connessione all'interfaccia SMTP Amazon SES utilizzando la riga di comando

I metodi descritti in questa sezione sono destinati a essere utilizzati dalla riga di comando per testare la connessione all'endpoint SMTP Amazon SES, convalidare le credenziali SMTP e risolvere i problemi di connessione. Queste procedure utilizzano strumenti e librerie inclusi nella maggior parte dei sistemi operativi più comuni.

Per ulteriori informazioni sulla risoluzione dei problemi di connessione SMTP, consulta Problemi relativi a SMTP in Amazon SES.

Prerequisiti

Quando ti connetti all'interfaccia SMTP Amazon SES devi fornire un set di credenziali SMTP. Queste credenziali SMTP sono diverse dalle credenziali standard. AWS I due tipi di credenziali non sono intercambiabili. Per ulteriori informazioni su come ottenere le credenziali SMTP, consulta the section called “Richiesta delle credenziali SMTP”.

Verifica della connessione all'interfaccia SMTP di Amazon SES

Puoi utilizzare la riga di comando per verificare la connessione all'interfaccia SMTP Amazon SES senza autenticare né inviare messaggi. Questa procedura è utile per la risoluzione dei problemi di connettività di base. Se la connessione di prova non riesce, consulta Problemi relativi a SMTP.

Questa sezione include le procedure per testare la connessione utilizzando sia OpenSSL (incluso nella maggior parte delle distribuzioni Linux, macOS e Unix ed è disponibile anche per Windows) sia `Test-NetConnection` il cmdlet PowerShell in (incluso nelle versioni più recenti di Windows).

Linux, macOS, or Unix

Esistono due modi per connettersi all'interfaccia SMTP Amazon SES con OpenSSL: utilizzando SSL esplicito sulla porta 587 o utilizzando SSL implicito sulla porta 465.

Connessione all'interfaccia SMTP utilizzando SSL esplicito

- Nella riga di comando, immetti il comando seguente per connetterti al server SMTP Amazon SES:

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

Nel comando precedente, sostituisci *email-smtp.us-west-2.amazonaws.com* con l'URL dell'endpoint SMTP Amazon SES per la tua regione. AWS Per ulteriori informazioni, consulta the section called “Regioni”.

Se la connessione è avvenuta correttamente, viene visualizzato un output simile al seguente:

```
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 connessione si chiude automaticamente dopo circa 10 secondi di inattività.

In alternativa, puoi utilizzare SSL implicito per connetterti all'interfaccia SMTP sulla porta 465.

Connessione all'interfaccia SMTP utilizzando SSL implicito

- Nella riga di comando, immetti il comando seguente per connetterti al server SMTP Amazon SES:

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

Nel comando precedente, sostituisci *email-smtp.us-west-2.amazonaws.com* con l'URL dell'endpoint SMTP Amazon SES per la tua regione. AWS Per ulteriori informazioni, consulta the section called “Regioni”.

Se la connessione è avvenuta correttamente, viene visualizzato un output simile al seguente:

```
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 connessione si chiude automaticamente dopo circa 10 secondi di inattività.

PowerShell

Puoi utilizzare il NetConnection cmdlet Test- PowerShell per connetterti al server SMTP Amazon SES.

> **Note**
>
> Il cmdlet `Test-NetConnection` può determinare se il computer è in grado di connettersi all'endpoint SMTP Amazon SES. Tuttavia, non verifica se il computer può effettuare una connessione SSL implicita o esplicita all'endpoint SMTP. Per testare una connessione SSL, è possibile installare OpenSSL per Windows per inviare un messaggio e-mail di prova.

Connessione all'interfaccia SMTP utilizzando il cmdlet **`Test-NetConnection`**

- Nel PowerShell, inserisci il seguente comando per connetterti al server SMTP Amazon SES:

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

Nel comando precedente, sostituisci *email-smtp.us-west-2.amazonaws.com* con l'URL dell'endpoint SMTP Amazon SES per la tua AWS regione e sostituisci *587* con il numero di porta. Per ulteriori informazioni sugli endpoint specifici di una Regione per Amazon SES, consulta the section called “Regioni”.

Se la connessione è avvenuta correttamente, viene visualizzato un output simile al seguente:

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

Utilizzo dell'API Amazon SES per l'invio di e-mail

Per inviare e-mail di produzione tramite Amazon SES, puoi utilizzare l'interfaccia Simple Mail Transfer Protocol (SMTP) o l'API Amazon SES. Per ulteriori informazioni sull'interfaccia SMTP, consulta Utilizzo dell'interfaccia SMTP Amazon SES per inviare e-mail. Questa sezione descrive come inviare e-mail utilizzando l'API.

Quando invii un messaggio di posta elettronica utilizzando l'API, puoi specificare il contenuto del messaggio e Amazon SES crea un'e-mail MIME per tuo conto. In alternativa, è possibile assemblare personalmente l'e-mail in modo da avere il controllo completo sul contenuto del messaggio. Per ulteriori informazioni sull'API di Amazon SES, consulta la Documentazione di riferimento delle API Amazon Simple Email Service. Per un elenco degli URL degli endpoint per i Regioni AWS quali è disponibile Amazon SES, consulta gli endpoint e le quote di Amazon Simple Email Service nel. Riferimenti generali di AWS

Puoi chiamare l'API nei modi seguenti:

- Richieste HTTPS dirette: questo è il metodo più avanzato perché è necessario gestire manualmente l'autenticazione e la firma delle richieste e quindi elaborare manualmente le richieste. Per ulteriori informazioni sull'API di Amazon SES, consulta la pagina di benvenuto della Documentazione di riferimento per API v2.
- Usa un AWS SDK:AWS gli SDK semplificano l'accesso alle API per diversi AWS servizi, incluso Amazon SES. Quando utilizzi un SDK, tale applicazione si occupa di autenticazione, richiesta di

accesso, logica relativa ai tentativi, gestione degli errori e altre funzioni di basso livello affinché tu possa concentrarti sulla creazione di applicazioni in grado di servire al meglio i tuoi clienti.

- Tramite un'interfaccia a riga di comando: AWS Command Line Interface è lo strumento a riga di comando di Amazon SES. Offriamo anche gli AWS strumenti PowerShell per coloro che eseguono script nell'ambiente. PowerShell

Indipendentemente dal fatto che tu acceda all'API di Amazon SES direttamente o indirettamente tramite un AWS SDK AWS Command Line Interface o gli AWS strumenti per PowerShell, l'API di Amazon SES offre due modi diversi per inviare un'e-mail, a seconda del livello di controllo che desideri sulla composizione del messaggio e-mail:

- Formattato: Amazon SES compone e invia un messaggio e-mail formattato correttamente. Devi solo specificare gli indirizzi di mittente e destinatario, un oggetto e un corpo del messaggio. Amazon SES si occupa di tutto il resto. Per ulteriori informazioni, consulta Invio di e-mail formattate mediante l'API Amazon SES.
- RAW: puoi comporre e inviare manualmente un messaggio e-mail, specificando intestazioni e-mail e tipi MIME personalizzati. Se hai esperienza nella formattazione delle tue e-mail, l'interfaccia RAW ti offre maggiore controllo sulla composizione del messaggio. Per ulteriori informazioni, consulta Invio di e-mail non elaborate utilizzando l'API Amazon SES v2.

Indice

Invio di e-mail formattate mediante l'API Amazon SES

Puoi inviare un'e-mail formattata utilizzando AWS Management Console o chiamando l'API Amazon SES tramite un'applicazione direttamente o indirettamente tramite un AWS SDK AWS Command Line Interface, il o il. AWS Tools for Windows PowerShell

L'API Amazon SES fornisce l'operazione `SendEmail`, che consente di comporre e inviare un messaggio e-mail formattato. `SendEmail` richiede indirizzo del mittente, indirizzo del destinatario,

oggetto e corpo del messaggio di testo, HTML o entrambi. Per ulteriori informazioni, consulta SendEmail(API Reference) o SendEmail(API v2 Reference).

> **Note**
>
> La stringa dell'indirizzo e-mail deve essere ASCII a 7 bit. Se desideri utilizzare indirizzi e-mail (del mittente o del destinatario) che contengono caratteri Unicode nella parte del dominio, devi codificare il dominio utilizzando Punycode. Per ulteriori informazioni, consulta il protocollo RFC 3492.

Per esempi su come comporre un messaggio formattato usando vari linguaggi di programmazione, consulta Esempi di codice.

Per suggerimenti su come aumentare la velocità di invio delle e-mail quando effettui più chiamate a `SendEmail`, consulta Aumento della velocità effettiva con Amazon SES.

Invio di e-mail non elaborate utilizzando l'API Amazon SES v2

Puoi utilizzare l'`SendEmail`operazione Amazon SES API v2 con il tipo di contenuto specificato `raw` per inviare messaggi personalizzati ai destinatari utilizzando il formato e-mail non elaborato.

Informazioni su campi di intestazione e-mail

SMTP (Simple Mail Transfer Protocol) specifica come devono essere inviati i messaggi e-mail definendo l'envelope del messaggio e-mail e alcuni dei relativi parametri senza fare riferimento al contenuto del messaggio. Il formato IMF (Internet Message Format) (RFC 5322) definisce invece il modo in cui il messaggio deve essere creato.

Con la specifica IMF, ogni messaggio e-mail è costituito da un'intestazione e un corpo. L'intestazione è costituita dai metadata del messaggio e il corpo contiene il messaggio. Per ulteriori informazioni su intestazione e corpo dei messaggi e-mail, consulta Formato dell'e-mail in Amazon SES.

Uso di MIME

Il protocollo SMTP è stato progettato per inviare messaggi e-mail che contengono solo caratteri ASCII a 7 bit. Questa specifica rende SMTP insufficiente per le codifiche di testo non ASCII (ad esempio Unicode), il contenuto binario o gli allegati. Lo standard MIME (Multipurpose Internet Mail Extensions) è stato sviluppato per rendere possibile l'invio di molti altri tipi di contenuti tramite il protocollo SMTP.

Lo standard MIME funziona suddividendo il corpo messaggio in più parti, quindi specificando cosa fare con ogni parte. Una parte del corpo di un messaggio e-mail può ad esempio essere costituita da testo semplice e un'altra può essere in formato HTML. MIME permette inoltre ai messaggi e-mail di contenere uno o più allegati. I destinatari dei messaggi possono visualizzare gli allegati dai propri client e-mail oppure possono salvarli.

L'intestazione del messaggio e il contenuto sono separati da una riga vuota. Ogni parte del messaggio e-mail è separata da una stringa di caratteri di delimitazione che indica l'inizio e la fine della parte.

Il messaggio in più parti nell'esempio seguente contiene una parte di testo, una parte HTML e un allegato. L'allegato va posizionato appena sotto alle intestazioni allegati ed è spesso codificato in `base64`, come mostrato in questo esempio.

```
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--
```

Il tipo di contenuto per il messaggio è `multipart/mixed`, che indica che il messaggio ha molte parti (in questo esempio, un corpo e un allegato) e che il client di ricezione deve gestire ogni parte separatamente.

Nidificata all'interno della sezione del corpo si trova una seconda parte, che usa il tipo di contenuto `multipart/alternative`. Questo tipo di contenuto indica che ogni parte include versioni alternative dello stesso contenuto (in questo caso, una versione di testo e una versione HTML). Se il client e-mail del destinatario è in grado di visualizzare contenuti HTML, viene visualizzata la versione HTML del corpo del messaggio. Se il client e-mail del destinatario non è in grado di visualizzare contenuti HTML, viene visualizzata la versione con testo normale del corpo del messaggio.

Entrambe le versioni del messaggio conterranno inoltre un allegato (in questo caso, un breve file di testo che contiene i nomi dei clienti).

Quando nidifichi una parte MIME all'interno di un'altra parte, come in questo esempio, la parte nidificata deve usare un parametro `boundary` distinto dal parametro `boundary` nella parte padre. Queste delimitazioni devono essere costituite da stringhe di caratteri univoche. Per definire una delimitazione tra parti MIME, digita due trattini (--) seguiti dalla stringa di delimitazione. Alla fine di una parte MIME, posiziona due trattini sia all'inizio che alla fine della stringa di delimitazione.

> **Note**
>
> Un messaggio non può contenere più di 500 parti MIME.

Codifica MIME

Per mantenere la compatibilità con i sistemi meno recenti, Amazon SES mantiene la limitazione ASCI a 7 bit di SMTP secondo quanto previsto dallo standard RFC 2821. Se desideri inviare contenuti che contengono caratteri non ASCII, devi codificare i caratteri in un formato che utilizza caratteri ASCII a 7 bit.

Indirizzi e-mail

La stringa dell'indirizzo e-mail deve essere ASCII a 7 bit. Se desideri utilizzare indirizzi e-mail (del mittente o del destinatario) che contengono caratteri Unicode nella parte del dominio, devi codificare il dominio utilizzando Punycode. Punycode non è consentito nella parte locale dell'indirizzo e-mail (ad esempio, la parte prima della @), né nel nome del mittente. Se desideri utilizzare caratteri Unicode nel nome del mittente, devi codificarlo con la sintassi MIME, come descritto in Invio di e-mail non elaborate utilizzando l'API Amazon SES v2. Per ulteriori informazioni su Punycode, consulta RFC 3492.

> **Note**
>
> Questa regola si applica solo agli indirizzi e-mail che specifichi nella busta del messaggio, non alle intestazioni dei messaggi. Quando utilizzi l'`SendEmail`operazione Amazon SES API v2, gli indirizzi specificati nei `Destinations` parametri `Source` e definiscono rispettivamente il mittente e il destinatario della busta.

Intestazioni dell'e-mail

Per codificare un messaggio, utilizza la sintassi codificata MIME. La sintassi codificata MIME usa il seguente formato:

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

Il valore di *`encoding`* può essere `Q` o `B`. Se il valore di codifica è `Q`, il valore *`encoded-text`* deve utilizzare il Q-encoding. Se il valore di codifica è `B`, il valore di *`encoded-text`* deve utilizzare la codifica base64.

Ad esempio, se vuoi utilizzare la stringa "Як ти поживаєш?" Nella riga dell'oggetto di un messaggio e-mail, puoi utilizzare le seguenti codificazioni:

- Q-encoding

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

- Codifica Base64

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

Per ulteriori informazioni sul Q-encoding, consulta RFC 2047. Per ulteriori informazioni sulla codifica base64, consulta RFC 2045.

Corpo del messaggio

Per codificare un messaggio, puoi utilizzare la codifica quoted-printable o la codifica Base64. Quindi, utilizza l'intestazione `Content-Transfer-Encoding` per indicare quale schema di codifica hai utilizzato.

Ad esempio, ipotizzando che il corpo del messaggio contenga il seguente testo:

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

Se scegli di codificare questo testo usando la codifica base64, devi prima specificare la seguente intestazione:

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

Quindi, nella sezione del corpo dell'e-mail, devi includere il testo con codifica base64:

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

> **Note**
>
> In alcuni casi, puoi utilizzare `Content-Transfer-Encoding` a 8 bit nei messaggi inviati utilizzando Amazon SES. Tuttavia, se Amazon SES deve apportare delle modifiche ai tuoi messaggi (ad esempio, quando utilizzi il monitoraggio di aperture e clic), i contenuti codificati a 8 bit potrebbero non comparire correttamente quando il messaggio raggiunge la casella della posta in arrivo del destinatario. Per questo motivo, è sempre consigliabile codificare i contenuti che non siano ASCII a 7 bit.

File allegati

Per allegare un file a un'e-mail, devi codificare l'allegato utilizzando la codifica base64. Gli allegati sono in genere posizionati nelle parti del messaggio MIME dedicate, le quali includono le seguenti intestazioni:

- Content-Type (Tipo di contenuto): il tipo di file dell'allegato. Di seguito sono elencati alcuni esempi comuni di dichiarazioni del tipo di contenuto MIME:
  - File di testo normale: `Content-Type: text/plain; name="sample.txt"`
  - Documento Microsoft Word: `Content-Type: application/msword; name="document.docx"`
  - Immagine JPG: `Content-Type: image/jpeg; name="photo.jpeg"`
- Content-Disposition (Disposizione del contenuto): specifica il modo in cui il client e-mail del destinatario deve gestire i contenuti. Per gli allegati, questo valore è `Content-Disposition: attachment`.
- Content-Transfer-Encoding (Codifica trasferimento del contenuto): lo schema utilizzato per codificare l'allegato. Per i file allegati, questo valore è quasi sempre `base64`.
- L'allegato codificato: è necessario codificare l'allegato vero e proprio e includerlo nel corpo sotto le intestazioni degli allegati, come mostrato nell'esempio.

Amazon SES accetta i tipi di file più comuni. Per un elenco dei tipi di file non accettati da Amazon SES, consulta Tipi di allegati non supportati di Amazon SES.

Invio di e-mail non elaborate utilizzando l'API Amazon SES v2

L'API Amazon SES v2 fornisce l'`SendEmail`azione, che consente di comporre e inviare un messaggio e-mail nel formato specificato quando si imposta il tipo di contenuto su semplice, non

elaborato o basato su modelli. Per una descrizione completa, consulta. `SendEmail` L'esempio seguente specificherà il tipo di contenuto `raw` per l'invio di messaggi utilizzando il formato e-mail non elaborato.

> **Note**
>
> Per suggerimenti su come aumentare la velocità di invio delle e-mail quando effettui più chiamate a `SendEmail`, consulta Aumento della velocità effettiva con Amazon SES.

Il corpo del messaggio deve contenere un messaggio e-mail in formato RAW formattato correttamente, con codifica appropriata per i campi di intestazione e il corpo del messaggio. Anche se è possibile creare il messaggio in formato RAW manualmente all'interno di un'applicazione, è molto più facile farlo usando le librerie di posta esistenti.

Java

Il seguente esempio di codice mostra come utilizzare la JavaMaillibreria e AWS SDK for Javacomporre e inviare un'e-mail non elaborata.

```
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

Il codice di esempio seguente illustra come usare i pacchetti Python email.mime e AWS SDK for Python (Boto) per comporre e inviare un messaggio e-mail in formato RAW.

```
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'])
```

Utilizzo di modelli per l'invio di e-mail personalizzate con l'API Amazon SES

È possibile utilizzare l'operazione CreateTemplateAPI per creare modelli di e-mail. che includano un oggetto, il testo e le parti HTML del corpo dell'e-mail. Le sezioni dell'oggetto e del corpo possono anche contenere valori univoci personalizzati per ogni destinatario.

Ci sono alcuni limiti e altre considerazioni da tenere presenti quando usi queste caratteristiche:

- Puoi creare fino a 20.000 modelli di email ciascuno Regione AWS.
- Ogni modello può raggiungere le dimensioni massime di 500 KB, inclusi testo e parti HTML.
- Puoi includere un numero illimitato di variabili di sostituzione in ogni modello.
- Puoi inviare e-mail a un massimo di 50 destinazioni in ciascuna chiamata all'operazione `SendBulkTemplatedEmail`. Una destinazione include un elenco di destinatari, nonché i destinatari "CC" e "BCC". Il numero di destinazioni che puoi contattare in una sola chiamata

all'API potrebbe essere limitato dalla frequenza massima in uscita del tuo account. Per ulteriori informazioni, consulta Gestione dei limiti di invio di Amazon SES.

Questa sezione include le procedure per la creazione di modelli di e-mail e per l'invio di e-mail personalizzate.

> **Note**
>
> Queste procedure si basano anche sul presupposto che l' AWS CLI sia già stata installata e configurata. Per ulteriori informazioni sull'installazione e la configurazione di AWS CLI, consulta la Guida per l'AWS Command Line Interface utente.

Fase 1: configurazione delle notifiche di eventi di errore di rendering

Se invii un'e-mail che contiene contenuti di personalizzazione non validi, Amazon SES potrebbe inizialmente accettare il messaggio, ma non sarà in grado di consegnarlo. Per questo motivo, se prevedi di inviare e-mail personalizzate, dovresti configurare Amazon SES in modo da inviare notifiche di eventi di errore di rendering tramite Amazon SNS. Quando ricevi una notifica di eventi di errore di rendering, puoi identificare il messaggio con i contenuti non validi, risolvere i problemi e inviare di nuovo il messaggio.

La procedura in questa sezione è opzionale, ma fortemente consigliata.

Configurazione delle notifiche di eventi di errore di rendering

1. Crea un argomento Amazon SNS. Per le istruzioni, consulta Creazione di un argomento nella Guida per gli sviluppatori di Amazon Simple Notification Service.
2. Iscriviti all'argomento Amazon SNS. Ad esempio, se desideri ricevere le notifiche di errore di rendering via e-mail, effettua la sottoscrizione di un endpoint di e-mail (ovvero il tuo indirizzo e-mail) all'argomento.

   Per le istruzioni, consulta Sottoscrizione a un argomento nella Guida per gli sviluppatori di Amazon Simple Notification Service.
3. Completa le procedure in the section called “Configurazione di una destinazione Amazon SNS” per impostare i set di configurazione per la pubblicazione degli eventi di errore di rendering nel tuo argomento Amazon SNS.

Fase 2: creazione di un modello di e-mail

In questa sezione, si utilizza l'operazione CreateTemplate API per creare un nuovo modello di e-mail con attributi di personalizzazione.

Questa procedura si basa sul presupposto che l' AWS CLI sia già stata installata e configurata. Per ulteriori informazioni sull'installazione e la configurazione di AWS CLI, consulta la Guida per l'AWS Command Line Interface utente.

Creazione del modello

1. In un editor di testo, crea un nuovo file. Incolla il codice seguente nel file.

```
{
  "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}}."
  }
}
```

   Questo codice contiene le seguenti proprietà:

   - TemplateName— Il nome del modello. Quando invii l'e-mail, fai riferimento a questo nome.
   - SubjectPart— La riga dell'oggetto dell'e-mail. Questa proprietà può contenere tag di sostituzione. Questi tag utilizzano il formato seguente: `{{tagname}}`. Quando invii l'e-mail, puoi specificare un valore `tagname` per ogni destinazione.

     L'esempio precedente include due tag: `{{name}}` e `{{favoriteanimal}}`.
   - HtmlPart— Il corpo HTML dell'e-mail. Questa proprietà può contenere tag di sostituzione.
   - TextPart— Il corpo del testo dell'e-mail. I destinatari i cui client e-mail non visualizzano e-mail in formato HTML vedranno questa versione del messaggio. Questa proprietà può contenere tag di sostituzione.
2. Personalizza l'esempio precedente in base alle tue esigenze, quindi salva il file come `mytemplate.json`.
3. Alla riga di comando, digita il comando seguente per creare un nuovo modello utilizzando l'operazione API `CreateTemplate`:

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

Fase 3: invio dell'e-mail personalizzata

Dopo aver creato un modello di e-mail, puoi utilizzarlo per l'invio di e-mail. Puoi utilizzare due operazioni API per inviare e-mail utilizzando modelli: `SendTemplatedEmail` e `SendBulkTemplatedEmail`. L'operazione `SendTemplatedEmail` è utile per l'invio di un'e-mail personalizzata a una singola destinazione (una raccolta di destinatari "A", "CC" e "BCC" che riceveranno la stessa e-mail). L'operazione `SendBulkTemplatedEmail` è utile per l'invio di e-mail univoche a più destinazioni in una singola chiamata all'API Amazon SES. Questa sezione fornisce esempi di come AWS CLI utilizzare l'invio di e-mail utilizzando entrambe queste operazioni.

Invio di un'e-mail basata su modello a una destinazione singola

Puoi utilizzare l'operazione `SendTemplatedEmail` per inviare un'e-mail a una destinazione singola. Tutti i destinatari nell'oggetto `Destination` riceveranno la stessa e-mail.

Invio di un'e-mail basata su modello a una destinazione singola

1. In un editor di testo, crea un nuovo file. Incolla il codice seguente nel file.

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

   Questo codice contiene le seguenti proprietà:

   - Source: l'indirizzo e-mail del mittente.
   - Template: il nome del modello da applicare all'e-mail.
   - ConfigurationSetNome: il nome del set di configurazione da utilizzare per l'invio dell'e-mail.

> **Note**
>
> È consigliabile utilizzare un set di configurazione configurato per pubblicare gli eventi di errore di rendering in Amazon SNS. Per ulteriori informazioni, consulta the section called “Fase 1: configurazione delle notifiche”.

- Destination: gli indirizzi dei destinatari. Puoi includere più indirizzi "A", "CC" e "BCC". Quando utilizzi l'operazione `SendTemplatedEmail`, tutti i destinatari ricevono la stessa e-mail.
- TemplateData— Una stringa JSON con escape che contiene coppie chiave-valore. Le chiavi corrispondono alle variabili nel modello (ad esempio, `{{name}}`). I valori rappresentano il contenuto che sostituisce le variabili nell'e-mail.

2. Modifica i valori nel codice precedente in base alle tue esigenze, quindi salva il file con il nome `myemail.json`.
3. Alla riga di comando, digita il seguente comando per inviare l'email:

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

Invio di un'e-mail basata su modello a più destinazioni

Puoi utilizzare l'operazione `SendBulkTemplatedEmail` per inviare un'e-mail a diverse destinazioni in un'unica chiamata all'API. Amazon SES invia un'e-mail univoca al destinatario o ai destinatari in ogni oggetto `Destination`.

Invio di un'e-mail basata su modello a più destinazioni

1. In un editor di testo, crea un nuovo file. Incolla il codice seguente nel file.

```
{
  "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\" }"
}
```

Questo codice contiene le seguenti proprietà:

- Source: l'indirizzo e-mail del mittente.
- Template: il nome del modello da applicare all'e-mail.
- ConfigurationSetNome: il nome del set di configurazione da utilizzare per l'invio dell'e-mail.

> **Note**
>
> È consigliabile utilizzare un set di configurazione configurato per pubblicare gli eventi di errore di rendering in Amazon SNS. Per ulteriori informazioni, consulta the section called “Fase 1: configurazione delle notifiche”.

- Destinations: una matrice che contiene una o più destinazioni.
  - Destination: gli indirizzi dei destinatari. Puoi includere più indirizzi "A", "CC" e "BCC". Quando utilizzi l'operazione `SendBulkTemplatedEmail`, tutti i destinatari nello stesso oggetto `Destination` ricevono la stessa e-mail.
  - ReplacementTemplateDati: un oggetto JSON che contiene coppie chiave-valore. Le chiavi corrispondono alle variabili nel modello (ad esempio, `{{name}}`). I valori rappresentano il contenuto che sostituisce le variabili nell'e-mail.
- DefaultTemplateDati: un oggetto JSON che contiene coppie chiave-valore. Le chiavi corrispondono alle variabili nel modello (ad esempio, `{{name}}`). I valori rappresentano il contenuto che sostituisce le variabili nell'e-mail. Questo oggetto contiene i dati di fallback. Se un oggetto `Destination` contiene un oggetto JSON vuoto nella proprietà `ReplacementTemplateData`, vengono utilizzati i valori della proprietà `DefaultTemplateData`.

2. Modifica i valori nel codice precedente in base alle tue esigenze, quindi salva il file con il nome `mybulkemail.json`.
3. Alla riga di comando, digita il seguente comando per inviare e-mail in blocco:

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

Personalizzazione avanzata dell'email

La funzione di modello in Amazon SES è basata sul sistema di modelli Handlebars. Puoi utilizzare Handlebars per creare modelli che includano caratteristiche avanzate, come attributi nidificati, iterazione di matrici, istruzioni condizionali di base e creazione di funzioni parziali in linea. In questa sezione vengono forniti alcuni esempi di queste caratteristiche.

Handlebars include altre caratteristiche oltre quelle documentate in questa sezione. Per ulteriori informazioni, consulta la pagina relativa agli Helper integrati in handlebarsjs.com.

> **Note**
>
> SES non fa l'escape del contenuto HTML durante il rendering del modello HTML per un messaggio. Ciò significa che se includi i dati inseriti dall'utente, ad esempio da un modulo di contatto, devi farne l'escape sul lato client.

Argomenti

Analisi degli attributi nidificati

Handlebars include il supporto per percorsi nidificati, semplificando la gestione dei dati complessi dei clienti e facendo quindi riferimento a quei dati nei tuoi modelli e-mail.

Per esempio, puoi organizzare i dati dei destinatari in diverse categorie generali. In ciascuna di quelle categorie, puoi includere informazioni dettagliate. L'esempio di codice che segue mostra un esempio di questa struttura per un singolo destinatario:

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

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

Nei tuoi modelli di e-mail, puoi riferirti agli attributi nidificati fornendo il nome dell'attributo padre, seguito da un punto (.), seguito dal nome dell'attributo per il quale si desidera includere il valore. Ad esempio, se utilizzi la struttura di dati illustrata nell'esempio precedente e desideri includere il nome di ciascun destinatario nel modello e-mail, includi il seguente testo nel tuo modello e-mail: `Hello {{contact.firstName}}!`

Handlebars è in grado di analizzare percorsi nidificati in diversi livelli, il che significa che disponi di una certa flessibilità nella modalità di strutturazione dei tuoi dati di modello.

Scorrimento degli elenchi

La funzione helper `each` scorre gli elementi in una matrice. Il codice seguente è un esempio di un modello e-mail che utilizza la funzione helper `each` per creare un elenco dettagliato degli interessi di ogni 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}}"
  }
}
```

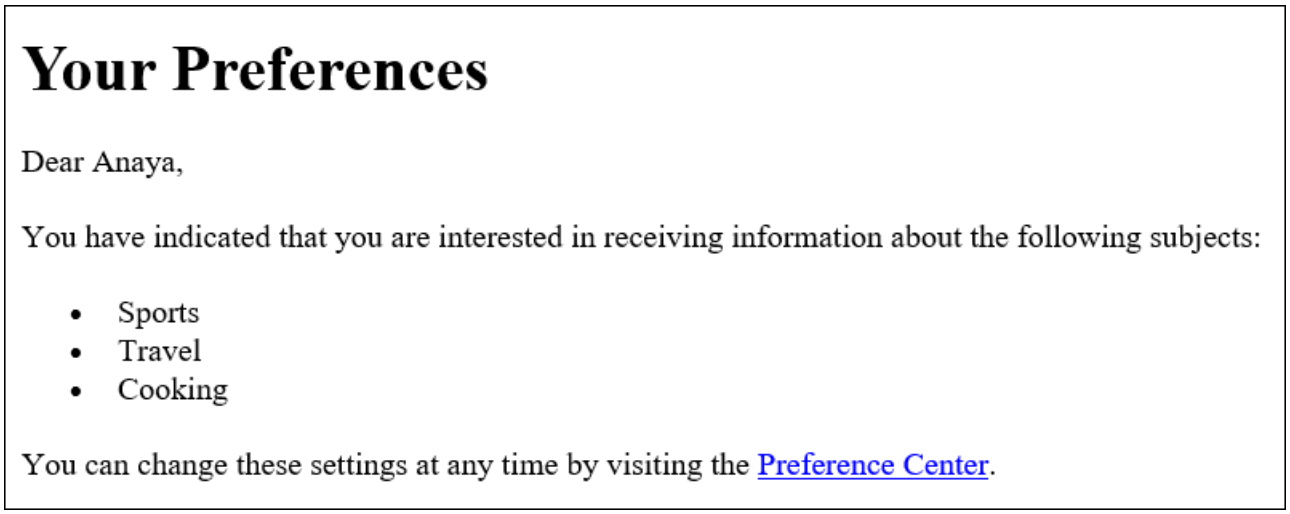
> **Important**
>
> Nel precedente esempio di codice, i valori degli attributi `HtmlPart` e `TextPart` includono interruzioni di riga per rendere più semplice la lettura dell'esempio. Il file JSON per il tuo modello non è in grado di contenere interruzioni di riga all'interno di questi valori. Se hai copiato e incollato questo esempio nel tuo file JSON, prima di procedere rimuovi le interruzioni di riga e gli spazi eccedenti dalle sezioni `HtmlPart` e `TextPart`.

Dopo che hai creato il modello, puoi utilizzare l'operazione `SendTemplatedEmail` o `SendBulkTemplatedEmail` per inviare e-mail ai destinatari utilizzando questo modello. Se ogni destinatario dispone di almeno un valore nell'oggetto `Interests`, questi ricevono un'e-mail che include un elenco dettagliato dei loro interessi. L'esempio seguente mostra un file JSON che può essere utilizzato per inviare e-mail a più destinatari utilizzando il modello precedente:

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

Quando invii un'e-mail ai destinatari elencati nell'esempio precedente utilizzando l'operazione `SendBulkTemplatedEmail`, questi ricevono un messaggio simile all'esempio illustrato nella seguente immagine:



Your Preferences

Dear Anaya,

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

- Sports
- Travel
- Cooking

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

Utilizzo di istruzioni condizionali di base

Questa sezione si basa sull'esempio descritto nella sezione precedente. L'esempio nella sezione precedente utilizza l'helper `each` per scorrere un elenco di interessi. Tuttavia, i destinatari per i quali non sono specificati interessi ricevono un'e-mail contenente un elenco vuoto. Utilizzando l'helper `{{if}}`, puoi formattare l'e-mail in modo diverso se un determinato attributo è presente nel modello dati. Il codice seguente utilizza l'helper `{{if}}` per visualizzare l'elenco puntato dalla sezione precedente se la matrice `Subscription` contiene qualsiasi valore. Se la matrice è vuota, viene visualizzato un altro blocco di testo.

```
{
  "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**
>
> Nel precedente esempio di codice, i valori degli attributi `HtmlPart` e `TextPart` includono interruzioni di riga per rendere più semplice la lettura dell'esempio. Il file JSON per il tuo modello non è in grado di contenere interruzioni di riga all'interno di questi valori. Se hai copiato e incollato questo esempio nel tuo file JSON, prima di procedere rimuovi le interruzioni di riga e gli spazi eccedenti dalle sezioni `HtmlPart` e `TextPart`.

L'esempio seguente mostra un file JSON che può essere utilizzato per inviare e-mail a più destinatari utilizzando il modello precedente:

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

In questo esempio il destinatario, il cui modello di dati ha incluso un elenco di interessi, riceve la stessa e-mail come l'esempio illustrato nella sezione precedente. Il destinatario con un modello di dati che non include alcun interesse, riceve comunque un'e-mail che somiglia all'esempio illustrato nella seguente immagine:

Creazione di funzioni parziali in linea

Puoi utilizzare funzioni parziali in linea per semplificare modelli che includono stringhe ripetute. Ad esempio, potresti creare una funzione in linea che include il nome del destinatario e, se è disponibile, il cognome aggiungendo il codice seguente all'inizio del tuo modello:

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

> **Note**
>
> Il carattere per la nuova riga (\n) è necessario per separare i blocchi `{{inline}}` dal contenuto nel tuo modello. Non viene eseguito il rendering della nuova riga nell'output finale.

Una volta creata la funzione parziale `fullName`, puoi includerla in qualsiasi punto del modello anteponendo al nome della parziale il segno "maggiore di" (>) seguito da uno spazio, come nell'esempio seguente: `{{> fullName}}`. Le funzioni parziali in linea non vengono trasferite tra le parti dell'e-mail. Ad esempio, se desideri utilizzare la stessa parziale in linea sia in HTML sia nella versione di testo dell'e-mail, è necessario definirla in entrambe le sezioni `HtmlPart` e `TextPart`.

Puoi utilizzare anche le funzioni parziali durante lo scorrimento delle matrici. Puoi utilizzare il codice seguente per creare un modello che usi la funzione parziale in linea `fullName`. In questo esempio, la parziale in linea si applica sia al nome del destinatario che a una vasta gamma di altri nomi:

```
{
  "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**
>
> Nel precedente esempio di codice, i valori degli attributi `HtmlPart` e `TextPart` includono interruzioni di riga per rendere più semplice la lettura dell'esempio. Il file JSON per il tuo modello non è in grado di contenere interruzioni di riga all'interno di questi valori. Se hai copiato e incollato questo esempio nel tuo file JSON, prima di procedere rimuovi le interruzioni di riga e gli spazi eccedenti da queste sezioni.

Gestione dei modelli e-mail

Oltre a creare modelli di e-mail puoi anche utilizzare l'API Amazon SES per aggiornare o eliminare i modelli esistenti, per pubblicare tutti i modelli esistenti o per visualizzare il contenuto di un modello.

Questa sezione contiene le procedure per l'utilizzo AWS CLI di per eseguire attività relative ai modelli Amazon SES.

> **Note**
>
> Queste procedure si basano anche sul presupposto che l' AWS CLI sia già stata installata e configurata. Per ulteriori informazioni sull'installazione e la configurazione di AWS CLI, consulta la Guida per l'AWS Command Line Interface utente.

Visualizzazione di un elenco di modelli e-mail

Puoi utilizzare l'ListTemplatesoperazione nell'API Amazon SES per visualizzare un elenco di tutti i modelli di e-mail esistenti.

Visualizzazione di un elenco di modelli e-mail

- Nella riga di comando, inserisci il comando seguente:

```
aws ses list-templates
```

Se nel tuo account Amazon SES sono presenti modelli di email nella Regione corrente, questo comando restituisce una risposta analoga all'esempio seguente:

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

Se non è stato creato alcun modello, il comando restituisce un `TemplatesMetadata` senza membri.

Visualizzazione del contenuto di un modello specifico di e-mail

Puoi utilizzare l'GetTemplateoperazione nell'API Amazon SES per visualizzare il contenuto di un modello di e-mail specifico.

Visualizzazione del contenuto di un modello di e-mail

- Nella riga di comando, inserisci il comando seguente:

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

  Nel comando precedente, *MyTemplate*sostituiscilo con il nome del modello che desideri visualizzare.

  Se il nome del modello fornito non corrisponde a un modello presente nel tuo account Amazon SES, il comando restituisce una risposta simile all'esempio seguente:

```
{
    "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>"
    }
}
```

  Se il nome del modello fornito non corrisponde a un modello presente nel tuo account Amazon SES, il comando restituisce un errore `TemplateDoesNotExist`.

Eliminazione di un modello di e-mail

Puoi utilizzare l'DeleteTemplateoperazione nell'API Amazon SES per eliminare un modello di e-mail specifico.

Eliminazione di un modello di e-mail

- Nella riga di comando, inserisci il comando seguente:

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

Nel comando precedente, *MyTemplate*sostituiscilo con il nome del modello che desideri eliminare.

Il comando non produce output. È possibile verificare che il modello sia stato eliminato utilizzando l'GetTemplateoperazione.

Aggiornamento di un modello di e-mail

Puoi utilizzare l'UpdateTemplateoperazione nell'API Amazon SES per aggiornare un modello di e-mail esistente. Ad esempio, questa operazione è utile se desideri modificare l'oggetto del modello di posta elettronica o devi modificare il corpo del messaggio stesso.

Aggiornamento di un modello di e-mail

1. Utilizza il comando `GetTemplate` per recuperare il modello esistente immettendo il seguente comando sulla riga di comando:

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

   Nel comando precedente, *MyTemplate*sostituiscilo con il nome del modello che desideri aggiornare.

   Se il nome del modello fornito non corrisponde a un modello presente nel tuo account Amazon SES, il comando restituisce una risposta simile all'esempio seguente:

   ```
   {
       "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. In un editor di testo, crea un nuovo file. Incolla l'output del comando precedente nel file.
3. Modifica il modello in base alle esigenze. Tutte le righe omesse vengono rimosse dal modello. Ad esempio, se desideri modificare solo la parte `SubjectPart` del modello, è comunque necessario includere le proprietà `TextPart` e `HtmlPart`.

Al termine, salva il file come `update_template.json`.

4. Nella riga di comando, inserisci il comando seguente:

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

Nel comando precedente, sostituisci *`path/to/update_template.json`* con il percorso al file `update_template.json` creato nella fase precedente.

Se il modello viene aggiornato correttamente, questo comando non fornisce alcun output. È possibile verificare che il modello sia stato aggiornato utilizzando l'GetTemplateoperazione.

Se il modello specificato non esiste, questo comando restituisce un errore `TemplateDoesNotExist`. Se il modello non contiene la proprietà `TextPart` o `HtmlPart` (o entrambe), questo comando restituisce un errore `InvalidParameterValue`.

Invio di e-mail tramite Amazon SES utilizzando un AWS SDK

Puoi utilizzare un AWS SDK per inviare e-mail tramite Amazon SES. AWS Gli SDK sono disponibili per diversi linguaggi di programmazione. Per ulteriori informazioni, consulta Strumenti per Amazon Web Services.

Prerequisiti

Per completare uno degli esempi di codice nella sezione successiva, è necessario completare i seguenti prerequisiti:

- Se non è già stato fatto, completa le attività in Impostazione di Amazon Simple Email Service.
- Verifica il tuo indirizzo e-mail con Amazon SES: prima di poter inviare un'e-mail con Amazon SES devi verificare di essere proprietario dell'indirizzo e-mail del mittente. Se il tuo account è ancora nella sandbox (ambiente di sperimentazione) Amazon SES, devi anche verificare l'indirizzo e-mail del destinatario. Ti consigliamo di utilizzare la console Amazon SES per verificare gli indirizzi e-mail. Per ulteriori informazioni, consulta Creazione di un'identità dell'indirizzo e-mail.
- Ottieni AWS le tue credenziali: sono necessari un ID chiave di AWS accesso e una chiave di accesso AWS segreta per accedere ad Amazon SES utilizzando un SDK. Per trovare le tue credenziali, usa la pagina Credenziali di sicurezza nell' AWS Management Console. Per ulteriori informazioni sulle credenziali, consulta Tipi di credenziali Amazon SES.

- Crea un file delle credenziali condiviso: per il corretto funzionamento del codice di esempio contenuto in questa sezione devi creare un file delle credenziali condiviso. Per ulteriori informazioni, consulta Creazione di un file di credenziali condiviso da utilizzare per l'invio di e-mail tramite Amazon SES utilizzando un SDK AWS.

Esempi di codice

> **Important**
>
> Nei seguenti tutorial invierai un'e-mail a te stesso, in modo da controllare se la ricevi. Per ulteriori sperimentazioni o per effettuare il test di carico, utilizza il simulatore di mailbox Amazon SES. Le e-mail inviate al simulatore di mailbox non vengono conteggiate ai fini della quota di invio o delle percentuali di mancati recapiti (bounce) e reclami. Per ulteriori informazioni, consulta Utilizzo manuale del simulatore di mailbox.

.NET

La procedura seguente mostra come inviare un'e-mail tramite Amazon SES utilizzando Visual Studio e AWS SDK for .NET.

Questa soluzione è stata testata con i seguenti componenti:

- Microsoft Visual Studio Community 2017, versione 15.4.0.
- Microsoft .NET Framework versione 4.6.1.
- Il pacchetto AWSSDK .Core (versione 3.3.19), installato utilizzando. NuGet
- Il AWSSDK. SimpleEmail pacchetto (versione 3.3.6.1), installato utilizzando. NuGet

Prima di iniziare, esegui queste attività:

- Installa Visual Studio: Visual Studio è disponibile all'indirizzo https://www.visualstudio.com/.

Per inviare un messaggio di posta elettronica utilizzando il AWS SDK for .NET

1. Crea un nuovo progetto seguendo i passaggi di seguito:

    a. Avvia Visual Studio.

b. Nel menu File scegli New (Nuovo), quindi Project (Progetto).

c. Nel pannello sinistro della finestra New Project (Nuovo progetto), espandi Installed (Installati), quindi espandi Visual C#.

d. Nel pannello destro, scegli Console App (.NET Framework) (App console (.NET Framework)).

e. In Name (Nome), digita **`AmazonSESSample`**, quindi scegli OK.

2. NuGet Utilizzalo per includere i pacchetti Amazon SES nella tua soluzione completando i seguenti passaggi:

a. Nel riquadro Solution Explorer, fai clic con il pulsante destro del mouse sul progetto, quindi scegli Gestisci NuGet pacchetti.

b. Nella scheda NuGet: AmazonsessAmple, scegli Sfoglia.

c. Nella casella di ricerca, digita **`AWSSDK.SimpleEmail`**.

d. Scegli il. AWSSDK SimpleEmailpacchetto, quindi scegli Installa.

e. Nella finestra Preview Changes (Anteprima modifiche), scegli OK.

3. Nella scheda Program.cs incolla il codice seguente:

```
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. Nell'editor del codice, procedi come segue:

   - Sostituisci *sender@example.com* con l'indirizzo e-mail del mittente. Questo indirizzo deve essere verificato. Per ulteriori informazioni, consulta Identità verificate.
   - Sostituisci *recipient@example.com* con l'indirizzo di destinazione. Se il tuo account si trova ancora nella sandbox (ambiente di sperimentazione), devi verificare anche quest'indirizzo.

- Sostituisci *ConfigSet*con il nome del set di configurazione da utilizzare per l'invio di questa e-mail.
- Sostituisci *USWest2* con il nome dell' Regione AWS endpoint che usi per inviare e-mail tramite Amazon SES. Per un elenco di regioni in cui Amazon SES è disponibile, consulta Amazon Simple Email Service (Amazon SES) in Riferimenti generali di AWS.

Al termine, salva `Program.cs`.

5. Compila ed esegui l'applicazione completando i passaggi seguenti:
   a. Nel menu Build (Compila), scegli Build Solution (Compila soluzione).
   b. Nel menu Debug scegli Start Debugging (Avvia debug). Viene visualizzata una finestra della console.
6. Verifica l'output della console. Se l'invio dell'e-mail è riuscito, la console visualizza "`The email was sent successfully.`"
7. Se l'e-mail è stata inviata correttamente, accedi al client e-mail dell'indirizzo del destinatario. Vedrai il messaggio inviato.

Java

La procedura seguente mostra come utilizzare Eclipse IDE per sviluppatori Java EE e come AWS Toolkit for Eclipsecreare un progetto AWS SDK e modificare il codice Java per inviare un'e-mail tramite Amazon SES.

Prima di iniziare, esegui queste attività:

- Installa Eclipse: Eclipse è disponibile all'indirizzo https://www.eclipse.org/downloads. Il codice in questo tutorial è stato testato usando Eclipse Neon.3 (versione 4.6.3), che esegue la versione 1.8 di Java Runtime Environment.
- Installa AWS Toolkit for Eclipse: le istruzioni per aggiungerlo AWS Toolkit for Eclipse alla tua installazione di Eclipse sono disponibili all'indirizzo https://aws.amazon.com/eclipse. Il codice in questo tutorial è stato testato usando la versione 2.3.1 di AWS Toolkit for Eclipse.

Per inviare un'e-mail utilizzando il AWS SDK for Java

1. Crea un progetto AWS Java in Eclipse eseguendo i seguenti passaggi:

a. Avvia Eclipse.

b. Dal menu File scegli New (Nuovo), quindi scegli Other (Altro). Nella finestra New (Nuovo) espandi la cartella AWS, quindi scegli AWS Java Project (Progetto Java AWS).

c. Nella finestra di dialogo Nuovo progetto AWS Java, effettuate le seguenti operazioni:

   i. Per Project name (Nome progetto), digita il nome di un progetto.

   ii. In AWS SDK for Java Esempi, seleziona Amazon Simple Email Service JavaMail Sample.

   iii. Scegli Finish (Fine).

2. In Eclipse, nel pannello Package Explorer, espandi il progetto.

3. All'interno del progetto, espandi la cartella `src/main/java`, espandi la cartella `com.amazon.aws.samples`, quindi fai doppio clic su `AmazonSESSample.java`.

4. Sostituisci l'intero contenuto di `AmazonSESSample.java` con il codice seguente:

```
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. In `AmazonSESSample.java`, sostituisci gli elementi seguenti con i tuoi valori:

> **Important**
>
> Gli indirizzi e-mail distinguono tra maiuscole e minuscole. Assicurati che gli indirizzi siano esattamente identici a quelli verificati.

- `SENDER@EXAMPLE.COM`: sostituisci con l'indirizzo e-mail del mittente. Devi verificare questo indirizzo prima di eseguire il programma. Per ulteriori informazioni, consulta Identità verificate in Amazon SES.
- `RECIPIENT@EXAMPLE.COM`: sostituisci con il tuo indirizzo e-mail del destinatario. Se il tuo account si trova ancora nella sandbox (ambiente di sperimentazione), devi verificare questo indirizzo prima di poterlo usare. Per ulteriori informazioni, consulta Richiedi l'accesso alla produzione (uscita dalla sandbox di Amazon SES).
- **`us-west-2`** (opzionale): per utilizzare Amazon SES in una Regione diversa da Stati Uniti occidentali (Oregon), sostituisci questo valore con la Regione che desideri utilizzare. Per un elenco di regioni in cui Amazon SES è disponibile, consulta Amazon Simple Email Service (Amazon SES) in Riferimenti generali di AWS.

6. Salva `AmazonSESSample.java`.
7. Per compilare il progetto, scegli Project (Progetto), quindi scegli Build Project (Compila progetto).

> **Note**
>
> Se questa opzione è disabilitata, è possibile che sia abilitata la compilazione automatica. In questo caso, ignora questa fase.

8. Per avviare il programma e inviare l'e-mail, scegli Run (Esegui), quindi di nuovo Run (Esegui).

9. Verifica l'output del pannello della console in Eclipse. Se l'e-mail è stata inviata correttamente, la console visualizza "`Email sent!`"; in caso contrario, viene visualizzato un messaggio di errore.
10. Se l'e-mail è stata inviata correttamente, accedi al client e-mail dell'indirizzo del destinatario. Vedrai il messaggio inviato.

PHP

Questo argomento mostra come utilizzare AWS SDK for PHP per inviare un'e-mail tramite Amazon SES.

Prima di iniziare, esegui queste attività:

- Installa PHP: PHP è disponibile all'indirizzo http://php.net/downloads.php. Questo tutorial richiede PHP versione 5.5 o successiva. Dopo aver installato PHP, aggiungi il relativo percorso alle variabili di ambiente in modo da poter eseguire PHP da qualsiasi prompt dei comandi. Il codice in questo tutorial è stato testato utilizzando PHP 7.2.7.
- Installa la AWS SDK for PHP versione 3: per le istruzioni di download e installazione, consulta la AWS SDK for PHP documentazione. Il codice in questo tutorial è stato testato utilizzando la versione 3.64.13 dell'SDK.

Per inviare un'e-mail tramite Amazon SES utilizzando AWS SDK for PHP

1. In un editor di testo crea un file denominato `amazon-ses-sample.php`. Incolla il codice seguente:

```
<?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. In `amazon-ses-sample.php`, sostituisci gli elementi seguenti con i tuoi valori:

   - **`path_to_sdk_inclusion`**—Sostituisci con il percorso richiesto per includerlo AWS SDK for PHP nel programma. Per ulteriori informazioni, consulta la documentazione relativa ad AWS SDK for PHP.
   - **`sender@example.com`**: sostituisci con un indirizzo e-mail verificato con Amazon SES. Per ulteriori informazioni, consulta Identità verificate. Gli indirizzi e-mail in Amazon SES distinguono tra maiuscole e minuscole. Assicurati che l'indirizzo inserito sia esattamente identico a quello verificato.
   - **`recipient1@example.com`**, **`recipient2@example.com`**: sostituisci con l'indirizzo del destinatario. Se il tuo account si trova ancora nella sandbox (ambiente di sperimentazione), deve essere verificato anche l'indirizzo del destinatario. Per ulteriori informazioni, consulta Richiedi l'accesso alla produzione (uscita dalla sandbox di Amazon SES). Assicurati che l'indirizzo inserito sia esattamente identico a quello verificato.
   - **`ConfigSet`** (opzionale): se desideri utilizzare un set di configurazione durante l'invio di questa e-mail, modifica il valore della variabile con il nome del set di configurazione. Per

ulteriori informazioni sui set di configurazione, consulta Utilizzo dei set di configurazione in Amazon SES.

- **`us-west-2`** (opzionale): per utilizzare Amazon SES in una Regione diversa da Stati Uniti occidentali (Oregon), sostituisci questo valore con la Regione che desideri utilizzare. Per un elenco di regioni in cui Amazon SES è disponibile, consulta Amazon Simple Email Service (Amazon SES) in Riferimenti generali di AWS.

3. Salva `amazon-ses-sample.php`.
4. Per eseguire il programma, apri un prompt dei comandi nella stessa directory di `amazon-ses-sample.php`, poi digita il seguente comando:

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

5. Esamina l'output. Se l'e-mail è stata inviata correttamente, la console visualizza "`Email sent!`"; in caso contrario, viene visualizzato un messaggio di errore.

> **Note**
>
> Se si verifica un errore "cURL error 60: SSL certificate problem" quando esegui il programma, scarica il bundle CA più recente, come descritto nella documentazione relativa ad AWS SDK for PHP. Quindi, in `amazon-ses-sample.php` aggiungi le seguenti righe alla matrice `SesClient::factory`, sostituisci `path_of_certs` con il percorso del bundle CA scaricato ed esegui nuovamente il programma.
>
> ```
> 'http' => [
>    'verify' => 'path_of_certs\ca-bundle.crt'
> ]
> ```

6. Accedi al client e-mail dell'indirizzo del destinatario. Vedrai il messaggio inviato.

Ruby

Questo argomento mostra come utilizzare AWS SDK for Ruby per inviare un'e-mail tramite Amazon SES.

Prima di iniziare, esegui queste attività:

- Installa Ruby: Ruby è disponibile all'indirizzo https://www.ruby-lang.org/en/downloads/. Il codice in questo tutorial è stato testato utilizzando Ruby 1.9.3. Dopo aver installato Ruby, aggiungi il

relativo percorso alle variabili di ambiente in modo da poter eseguire Ruby da qualsiasi prompt dei comandi.

- Installa il AWS SDK for Ruby —Per le istruzioni di download e installazione, consulta Installazione di AWS SDK for Ruby nella Guida per gli AWS SDK for Ruby sviluppatori. Il codice di esempio di questo tutorial è stato testato utilizzando la versione 2.9.36 di AWS SDK for Ruby.
- Crea un file delle credenziali condiviso: per il corretto funzionamento del codice di esempio contenuto in questa sezione devi creare un file delle credenziali condiviso. Per ulteriori informazioni, consulta Creazione di un file di credenziali condiviso da utilizzare per l'invio di e-mail tramite Amazon SES utilizzando un SDK AWS.

Per inviare un'e-mail tramite Amazon SES utilizzando AWS SDK for Ruby

1. In un editor di testo crea un file denominato `amazon-ses-sample.rb`. Incolla il codice seguente nel file:

```
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. In `amazon-ses-sample.rb`, sostituisci gli elementi seguenti con i tuoi valori:

   - **`sender@example.com`**: sostituisci con un indirizzo e-mail verificato con Amazon SES. Per ulteriori informazioni, consulta Identità verificate. Gli indirizzi e-mail in Amazon SES distinguono tra maiuscole e minuscole. Assicurati che l'indirizzo inserito sia esattamente identico a quello verificato.
   - **`recipient@example.com`**: sostituisci con l'indirizzo del destinatario. Se il tuo account si trova ancora nella sandbox (ambiente di sperimentazione), devi verificare questo indirizzo prima di poterlo usare. Per ulteriori informazioni, consulta Richiedi l'accesso alla produzione (uscita dalla sandbox di Amazon SES). Assicurati che l'indirizzo inserito sia esattamente identico a quello verificato.
   - **`us-west-2`** (opzionale): per utilizzare Amazon SES in una Regione diversa da Stati Uniti occidentali (Oregon), sostituisci questo valore con la Regione che desideri utilizzare. Per un elenco di regioni in cui Amazon SES è disponibile, consulta Amazon Simple Email Service (Amazon SES) in Riferimenti generali di AWS.
3. Salva `amazon-ses-sample.rb`.
4. Per eseguire il programma, apri un prompt dei comandi nella stessa directory di `amazon-ses-sample.rb`, quindi digita ruby amazon-ses-sample.rb
5. Esamina l'output. Se l'e-mail è stata inviata correttamente, la console visualizza "`Email sent!`"; in caso contrario, viene visualizzato un messaggio di errore.
6. Accedi al client e-mail dell'indirizzo del destinatario. Troverai il messaggio inviato.

Python

Questo argomento mostra come utilizzare AWS SDK for Python (Boto) per inviare un'e-mail tramite Amazon SES.

Prima di iniziare, esegui queste attività:

- Verifica il tuo indirizzo e-mail con Amazon SES: prima di poter inviare un'e-mail con Amazon SES devi verificare di essere proprietario dell'indirizzo e-mail del mittente. Se il tuo account

è ancora nella sandbox (ambiente di sperimentazione) Amazon SES, devi anche verificare l'indirizzo e-mail del destinatario. Ti consigliamo di utilizzare la console Amazon SES per verificare gli indirizzi e-mail. Per ulteriori informazioni, consulta Creazione di un'identità dell'indirizzo e-mail.

- Ottieni AWS le tue credenziali: sono necessari un ID chiave di AWS accesso e una chiave di accesso AWS segreta per accedere ad Amazon SES utilizzando un SDK. Per trovare le tue credenziali, usa la pagina Credenziali di sicurezza nell' AWS Management Console. Per ulteriori informazioni sulle credenziali, consulta Tipi di credenziali Amazon SES.
- Installa Python: Python è disponibile all'indirizzo https://www.python.org/downloads/. Il codice in questo tutorial è stato testato utilizzando Python 2.7.6 e Python 3.6.1. Dopo aver installato Python, aggiungi il relativo percorso alle variabili di ambiente in modo da poter eseguire Python da qualsiasi prompt dei comandi.
- Installa AWS SDK for Python (Boto): per le istruzioni di download e installazione, consulta la documentazione.AWS SDK for Python (Boto) Il codice di esempio di questo tutorial è stato testato utilizzando la versione 1.4.4 dell'SDK for Python.

Invio di un'e-mail tramite Amazon SES utilizzando SDK for Python

1. In un editor di testo crea un file denominato `amazon-ses-sample.py`. Incolla il codice seguente nel file:

```
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. In `amazon-ses-sample.py`, sostituisci gli elementi seguenti con i tuoi valori:

   - **`sender@example.com`**: sostituisci con un indirizzo e-mail verificato con Amazon SES. Per ulteriori informazioni, consulta Identità verificate. Gli indirizzi e-mail in Amazon SES distinguono tra maiuscole e minuscole. Assicurati che l'indirizzo inserito sia esattamente identico a quello verificato.
   - **`recipient@example.com`**: sostituisci con l'indirizzo del destinatario. Se il tuo account si trova ancora nella sandbox (ambiente di sperimentazione), devi verificare questo indirizzo prima di poterlo usare. Per ulteriori informazioni, consulta Richiedi l'accesso alla produzione (uscita dalla sandbox di Amazon SES). Assicurati che l'indirizzo inserito sia esattamente identico a quello verificato.
   - **`us-west-2`** (opzionale): per utilizzare Amazon SES in una Regione diversa da Stati Uniti occidentali (Oregon), sostituisci questo valore con la Regione che desideri utilizzare. Per un elenco di regioni in cui Amazon SES è disponibile, consulta Amazon Simple Email Service (Amazon SES) in Riferimenti generali di AWS.

3. Salva `amazon-ses-sample.py`.

4. Per eseguire il programma, apri un prompt dei comandi nella stessa directory di `amazon-ses-sample.py`, poi digita python amazon-ses-sample.py.
5. Esamina l'output. Se l'e-mail è stata inviata correttamente, la console visualizza "`Email sent!`"; in caso contrario, viene visualizzato un messaggio di errore.
6. Accedi al client e-mail dell'indirizzo del destinatario. Vedrai il messaggio inviato.

Creazione di un file di credenziali condiviso da utilizzare per l'invio di e-mail tramite Amazon SES utilizzando un SDK AWS

La procedura seguente mostra come creare un file delle credenziali condiviso nella directory principale. Per il corretto funzionamento del codice di esempio SDK, è necessario creare il file.

1. In un editor di testo, crea un nuovo file. Nel file incolla il codice seguente:

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

2. Nel file di testo appena creato, sostituiscilo `YOUR_AWS_ACCESS_KEY` con l'ID della tua chiave di AWS accesso univoca e sostituiscilo `YOUR_AWS_SECRET_ACCESS_KEY` con la tua chiave di accesso AWS segreta univoca.
3. Salva il file. La tabella seguente mostra il percorso e il nome di file corretti per il sistema operativo.

Se usi...	Salva il file come...
Windows	`C:\Users\<yourUserName>\.aws\credentials`
Linux, macOS o Unix	`~/.aws/credentials`

> **Important**
>
> Non includere l'estensione del file quando salvi il file delle credenziali.

Codifiche dei contenuti supportate da Amazon SES

Le seguenti informazioni sono fornite per riferimento.

Amazon SES supporta le seguenti codifiche dei contenuti:

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

Amazon SES supporta anche il formato di intestazione Accept-Encoding seguente, in base alla specifica 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`

Protocolli di sicurezza e Amazon SES

Questo argomento descrive i protocolli di sicurezza che puoi utilizzare quando ti connetti ad Amazon SES e quando Amazon SES consegna un'e-mail a un ricevitore.

Mittente dell'e-mail ad Amazon SES

Il protocollo di sicurezza da usare per connetterti ad Amazon SES dipende da cosa utilizzi, se l'API Amazon SES o l'interfaccia SMTP Amazon SES, come descritto di seguito.

HTTPS

Se utilizzi l'API Amazon SES (direttamente o tramite un AWS SDK), tutte le comunicazioni vengono crittografate tramite TLS tramite l'endpoint HTTPS di Amazon SES. L'endpoint HTTPS Amazon SES supporta TLS 1.2 e TLS 1.3.

Interfaccia SMTP

Se accedi ad Amazon SES tramite l'interfaccia SMTP, devi crittografare la connessione utilizzando Transport Layer Security (TLS). Nota che TLS è spesso indicato con il nome del suo predecessore, il protocollo Secure Sockets Layer (SSL).

Amazon SES supporta due meccanismi per stabilire una connessione crittografata tramite TLS: STARTTLS e TLS Wrapper.

- STARTTLS: STARTTLS consente di aggiornare una connessione non crittografata in una connessione crittografata. Esistono versioni di STARTTLS per diversi protocolli; la versione SMTP è definita nello standard RFC 3207. Per le connessioni STARTTLS, Amazon SES supporta TLS 1.2 e TLS 1.3.
- TLS Wrapper: TLS Wrapper, noto anche come SMTPS o protocollo Handshake, consente di avviare una connessione crittografata senza prima stabilire una connessione non crittografata. Con TLS Wrapper, l'endpoint SMTP Amazon SES non esegue la negoziazione TLS, ma spetta al client connettersi all'endpoint tramite TLS e continuare a usare TLS per l'intera conversazione. TLS Wrapper è un protocollo meno recente, ma è supportato da molti client. Per le connessioni TLS Wrapper, Amazon SES supporta TLS 1.2 e TLS 1.3.

Per informazioni sulla connessione all'interfaccia SMTP Amazon SES utilizzando questi metodi, consulta Connessione a un endpoint SMTP Amazon SES.

Da Amazon SES al destinatario

SES supporta TLS 1.2 per le connessioni TLS. Per ulteriori informazioni, consulta Sicurezza dell'infrastruttura in SES.

Per impostazione predefinita, Amazon SES utilizza TLS opportunistico. Questo significa che Amazon SES tenta sempre di effettuare una connessione sicura al server di posta di ricezione. Se Amazon SES non è in grado di stabilire una connessione sicura, invia il messaggio non crittografato.

È possibile modificare questo comportamento utilizzando i set di configurazione. Utilizza l'operazione PutConfigurationSetDeliveryOptions API per impostare la `TlsPolicy` proprietà per una configurazione impostata su. `Require` È possibile utilizzare AWS CLI per apportare questa modifica.

Configurazione di Amazon SES in modo da richiedere connessioni TLS per un set di configurazione

- Nella riga di comando, inserisci il comando seguente:

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

Nell'esempio precedente, *MyConfigurationsostituite Set* con il nome del set di configurazione.

Quando invii un'e-mail utilizzando questo set di configurazione, Amazon SES invia il messaggio al server e-mail di ricezione solo se è in grado di stabilire una connessione sicura. Se Amazon SES non è in grado di effettuare una connessione sicura al server e-mail di ricezione, elimina il messaggio.

Crittografia E nd-to-end

È possibile utilizzare Amazon SES per inviare messaggi crittografati utilizzando S/MIME o PGP. I messaggi che utilizzano questi protocolli vengono crittografati dal mittente. I contenuti possono essere visualizzati solo dai destinatari che possiedono le chiavi private necessarie per decrittare i messaggi.

Amazon SES supporta i seguenti tipi MIME, che è possibile utilizzare per l'invio di e-mail crittografate S/MIME:

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

Amazon SES supporta anche i seguenti tipi MIME, che è possibile utilizzare per l'invio di e-mail PGP crittografate:

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

Campi di intestazione Amazon SES

Amazon SES può accettare qualsiasi intestazione di e-mail che segua il formato descritto in RFC 822.

I seguenti campi non possono essere visualizzati più di una volta nella sezione di intestazione di un messaggio:

- `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`

Considerazioni

- Questo campo `acceptLanguage` è non standard. Se possibile, utilizzare l'intestazione `Accept-Language`.
- Se specifichi un'intestazione `Date`, Amazon SES la sostituisce con un timestamp corrispondente alla data e all'ora nel fuso orario UTC quando Amazon SES ha accettato il messaggio.
- Se fornisci un'intestazione `Message-ID`, Amazon SES sostituisce l'intestazione con il suo valore.
- Se specifichi un'intestazione `Return-Path`, Amazon SES invia notifiche di mancato recapito (bounce) e di reclamo all'indirizzo specificato. Tuttavia, il messaggio ricevuto dai destinatari contiene un valore diverso per l'intestazione `Return-Path`.
- Se utilizzi l'`SendEmail`operazione Amazon SES API v2 con contenuto semplice o basato su modelli o utilizzi l'*`SendBulkEmail`*operazione, non puoi impostare contenuti di intestazione personalizzati per le intestazioni impostate da SES; pertanto, le seguenti intestazioni non sono consentite come intestazioni personalizzate:
  - `BCC`, `CC`, `Content-Disposition`, `Content-Type`, `Date`, `From`, `Message-ID`, `MIME-Version`, `Reply-To`, `Return-Path`, `Subject`, `To`

Tipi di allegati non supportati di Amazon SES

È possibile inviare messaggi con allegati tramite Amazon SES utilizzando lo standard Multipurpose Internet Mail Extensions (MIME). Amazon SES accetta come allegati tutti i tipi di file eccetto gli allegati con le estensioni riportate nell'elenco seguente.

.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

Alcuni ISP presentano restrizioni ulteriori (ad esempio restrizioni riguardanti gli allegati archiviati), per cui ti consigliamo di testare l'e-mail effettuando invii attraverso gli ISP principali prima di inviare e-mail di produzione.

Ricezione di e-mail con Amazon SES

Oltre a utilizzare Amazon SES per gestire l'invio di e-mail, puoi anche configurare SES per ricevere e-mail per conto di uno o più dei tuoi domini. In quanto ricevitore di e-mail, SES gestisce le operazioni di ricezione di e-mail sottostanti, ad esempio la comunicazione con altri server di posta, la scansione alla ricerca di spam e virus, il rifiuto di posta proveniente da origini non attendibili (indirizzi presenti negli elenchi di indirizzi bloccati Spamhaus o SES) e l'accettazione di posta per i destinatari nel dominio.

L'entità dell'elaborazione dell'e-mail ricevuta è determinata dalle istruzioni personalizzate specificate. Queste istruzioni sono disponibili in due forme:

- Le regole di ricezione (controllo basato sul destinatario) forniscono la massima granularità di controllo sulla posta elettronica in arrivo. Le regole di ricezione possono eseguire l'elaborazione avanzata, ad esempio consegnare la posta in arrivo a un bucket Amazon S3, pubblicarla su un argomento Amazon SNS, inviarla ad Amazon WorkMail o inviare automaticamente messaggi di mancato recapito quando i messaggi sono inviati a indirizzi e-mail specifici e altro ancora.
- I filtri per indirizzi IP (controllo basato su IP) forniscono un ampio livello di controllo e sono semplici da configurare. Questi filtri consentono di bloccare o consentire esplicitamente tutti i messaggi provenienti da indirizzi IP o intervalli di indirizzi IP specifici.

Per iniziare a conoscere la ricezione delle e-mail, la configurazione e l'implementazione utilizzando regole di ricezione o filtri per indirizzi IP, per prima cosa leggi Concetti di ricezione e-mail e casi d'uso per avere una panoramica di come funziona e dei diversi modi in cui è possibile utilizzarlo. Quindi, Configurazione della ricezione di e-mail ti guiderà attraverso i prerequisiti di configurazione per la ricezione dell'e-mail. Quindi, Spiegazioni passo per passo sulla console di ricezione di e-mail ti guiderà attraverso le procedure guidate utilizzate per configurare regole di ricezione e filtri per indirizzi IP.

> **Note**
>
> La ricezione di e-mail può essere utilizzata solo se l'account si trova in una Regione AWS in cui SES supporta la ricezione di e-mail. Consulta la sezione SES supported email receiving regions (Regioni supportate da SES per la ricezione di e-mail).

Argomenti in questa sezione:

Concetti di ricezione e-mail Amazon SES e casi d'uso

Quando scegli Amazon SES come ricevitore di e-mail, devi indicare al servizio come gestire la tua posta. Il metodo principale, ossia le regole di ricezione, offre un controllo granulare sulla ricezione dell'e-mail utilizzando un controllo basato sul destinatario per specificare una serie di azioni da eseguire in base al destinatario. L'altro metodo, i filtri degli indirizzi IP, fornisce un ampio livello di controllo basato su IP per bloccare o consentire la posta in base all'indirizzo IP o all'intervallo di indirizzi di origine.

Entrambi questi metodi sono descritti in questa sezione insieme a una panoramica di come Amazon SES elabora le e-mail ricevute e i casi d'uso per aiutarti a considerare come intendi ricevere, filtrare ed elaborare la tua posta elettronica durante l'impostazione di regole e filtri.

Argomenti in questa sezione:

Controllo basato sul destinatario mediante regole di ricezione

Il modo principale per controllare la posta in arrivo consiste in specificare la modalità di gestione della posta tramite un elenco ordinato di operazioni per le identità di dominio verificate che include domini, domini secondari o indirizzi e-mail che appartengono a una delle identità di dominio verificate. Queste azioni sono definite e ordinate in regole di ricezione che crei all'interno di un set di regole.

In alternativa, è possibile aggiungere condizioni di ricezione per specificare che le operazioni vengano eseguite solo se il destinatario della posta in entrata corrisponde a un'identità specificata

nella condizione. Ad esempio, se sei titolare di example.com, puoi specificare che la posta per user@example.com non deve essere recapitata e che tutti gli altri messaggi per example.com e i relativi sottodomini devono essere consegnati.

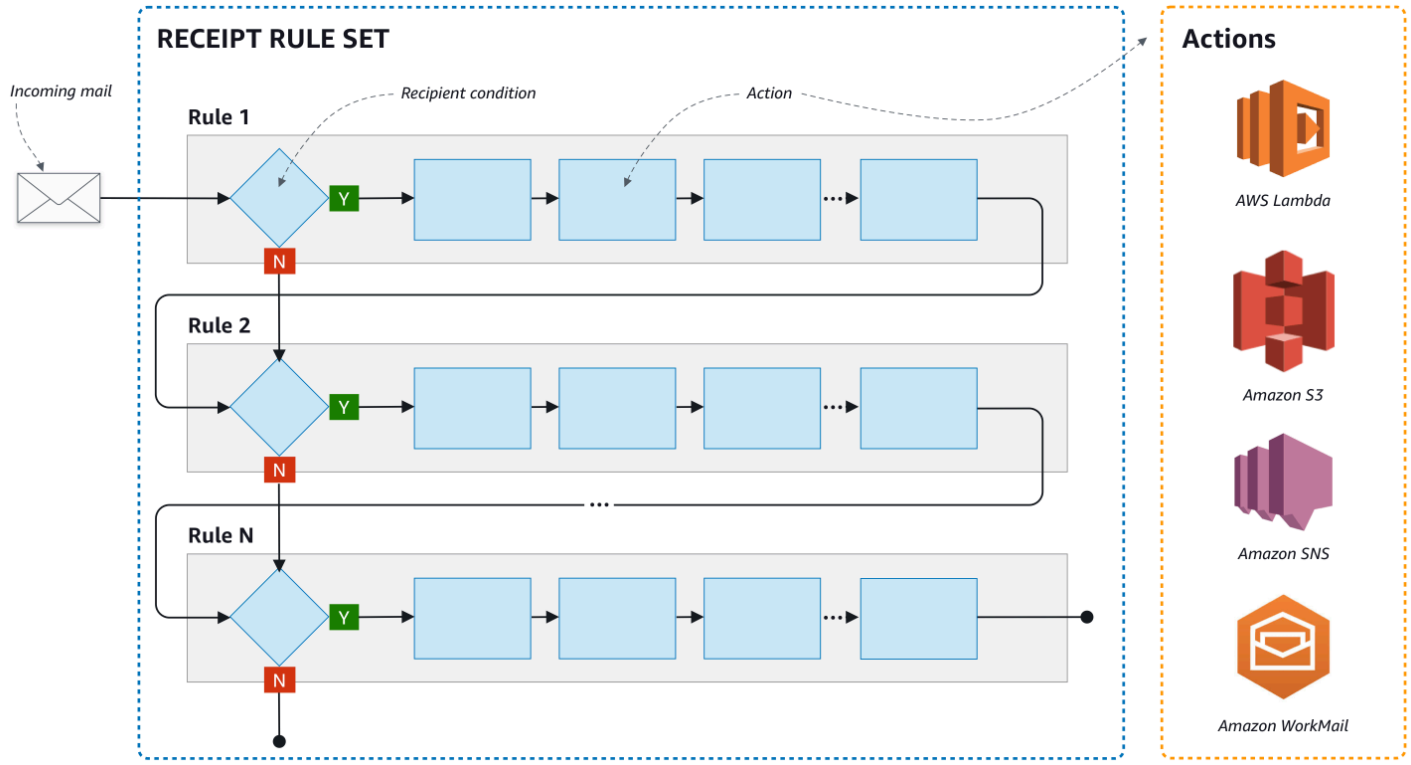
In caso contrario, se non si aggiungono condizioni di destinatario, le azioni verranno applicate a tutti gli indirizzi e-mail, i domini e i sottodomini che appartengono ai domini verificati. Alle regole di ricezione possono essere applicate le seguenti azioni disponibili:

- Add header action (Operazione di aggiunta intestazione): aggiunge un'intestazione all'e-mail ricevuta. Questa operazione viene generalmente utilizzata solo in combinazione con altre.
- Operazione di restituzione risposta di mancato recapito: blocca l'e-mail restituendo una risposta di mancato recapito al mittente e, opzionalmente, ti invia una notifica tramite Amazon SNS.
- Invoke AWS Lambda function action (Operazione di richiamo funzione AWS Lambda): chiama il codice tramite una funzione Lambda e, opzionalmente, ti invia una notifica tramite Amazon SNS.
- Deliver to S3 bucket action (Operazione di consegna a bucket S3): consegna la posta a un bucket Amazon S3 e, opzionalmente, ti invia una notifica tramite Amazon SNS.
- Publish to Amazon SNS topic action (Operazione di pubblicazione in argomento Amazon SNS): pubblica l'e-mail completa in un argomento Amazon SNS.

  > **Note**
  >
  > L'operazione SNS include una copia completa del contenuto delle e-mail nelle notifiche Amazon SNS. Le altre notifiche Amazon SNS menzionate qui servono semplicemente a notificare la consegna dell'e-mail; contengono informazioni sull'e-mail e non sul relativo contenuto.

- Stop rule set action (Operazione di interruzione set di regole): termina la valutazione del set di regole di ricezione e, opzionalmente, ti invia una notifica tramite Amazon SNS.
- Integrate with Amazon WorkMail action (Operazione di integrazione con Amazon WorkMail): gestisce la posta con Amazon WorkMail. In genere, questa operazione non viene utilizzata direttamente perché Amazon WorkMail si occupa della configurazione.

Le regole di ricezione sono raggruppate in set di regole. Se non disponi di un set di regole esistente, sarà necessario creare un set di regole prima di iniziare a creare regole di ricezione. Puoi definire più set di regole di ricezione per il tuo account AWS, ma solo un set alla volta può essere attivo. La figura seguente mostra l'interrelazione tra regole di ricezione, set di regole di ricezione e operazioni.



Controllo basato su IP mediante filtri di indirizzi IP

Puoi tenere sotto controllo il flusso di posta impostando filtri per indirizzi IP. I filtri per indirizzi IP sono opzionali e consentono di specificare se accettare o bloccare la posta proveniente da un indirizzo IP o un intervallo di indirizzi IP. I tuoi filtri per indirizzi IP possono includere elenchi di indirizzi bloccati (indirizzi IP da cui bloccare la posta in entrata) ed elenchi di indirizzi consentiti (indirizzi IP da cui desideri sempre accettare la posta).

I filtri per indirizzi IP sono utili per bloccare i messaggi spam. Amazon SES gestisce il proprio elenco di indirizzi IP bloccati noti per l'invio di spam, inclusi quelli elencati in Spamhaus. Tuttavia, è possibile scegliere di ricevere posta da tali indirizzi IP aggiungendoli al proprio elenco di indirizzi consentiti. Poiché non ci sono registri che indicano quali indirizzi IP vengono bloccati, il mittente bloccato dovrà informare l'utente. Questa è anche una buona opportunità per aiutare il mittente a determinare se il proprio indirizzo IP si trova in un elenco di indirizzi bloccati, ad esempio Spamhaus e consigliare di richiedere di essere rimossi dall'elenco. Ciò sarà utile sia per te che per il mittente in quanto non dovrai gestire un filtro degli indirizzi IP per suo conto e migliorerà il suo tasso di recapito delle e-mail.

> **Note**
>
> - Indipendentemente dalla configurazione del filtro dell'indirizzo IP, Amazon EC2 bloccherà il traffico in uscita sulla porta 25 (invio di posta), a meno che non sia elencato come consentito. Fai riferimento a questo articolo di AWS Re:POST per ulteriori informazioni.
> - Se desideri ricevere la posta solo da un elenco limitato di indirizzi IP noti, configura un elenco di indirizzi bloccati contenente `0.0.0.0/0` e un elenco di indirizzi permessi contenente gli indirizzi IP attendibili. Questa configurazione blocca tutti gli indirizzi IP per impostazione predefinita e permette la ricezione di posta solo dagli indirizzi IP specificati in modo esplicito.

Processo di ricezione di e-mail

Quando Amazon SES riceve un'e-mail per il tuo dominio, si verificano i seguenti eventi:

1. Amazon SES esamina innanzitutto l'indirizzo IP del mittente. Amazon SES consente al messaggio di superare questa fase a meno che:
   - l'indirizzo IP sia presente nel tuo elenco di indirizzi bloccati;
   - l'indirizzo IP sia presente nell'elenco di indirizzi bloccati di Amazon SES e non sia incluso nel tuo elenco di indirizzi consentiti.
2. Amazon SES esamina il set di regole di ricezione attivo per determinare se le regole contengano una condizione di ricezione:
   - Se c'è una condizione del destinatario e corrisponde a uno qualsiasi dei destinatari dell'e-mail in arrivo, Amazon SES accetta l'e-mail. In caso contrario, se non vi sono corrispondenze, Amazon SES blocca l'e-mail.
   - Se la regola di ricezione non contiene una condizione del destinatario, Amazon SES accetta la posta; tutte le azioni della regola verranno applicate a tutte le identità verificate di cui sei proprietario.
3. Amazon SES autentica l'e-mail e ne analizza il contenuto alla ricerca di spam e malware:
   - L'indirizzo IP dell'host remoto che ha inviato l'e-mail ad Amazon SES viene controllato in base alla policy SPF specificata nel dominio di MAIL FROM utilizzato durante la transazione SMTP.
   - Le firme DKIM presenti nella sezione di intestazione dell'e-mail sono controllate.
   - Se la scansione dei contenuti è abilitata, il contenuto dell'e-mail viene analizzato alla ricerca di spam e malware.

- I risultati dell'autenticazione dell'e-mail e della scansione del contenuto vengono resi disponibili durante la valutazione delle regole di ricezione.

Per ulteriori informazioni, consulta Autenticazione di e-mail e rilevamento malware.

4. Per l'e-mail che Amazon SES accetta, tutte le regole di ricezione all'interno del set di regole attivo vengono applicate nell'ordine definito e, all'interno di ogni regola di ricezione, le operazioni vengono eseguite nell'ordine definito.

Casi d'uso e restrizioni per la ricezione di e-mail con Amazon SES

Questa sezione esamina alcune considerazioni generali e casi d'uso per la ricezione di e-mail con Amazon SES. Presentate sotto forma di domande e risposte, sono riportate le domande frequenti e i fatti per determinare se è vantaggioso utilizzare Amazon SES per ricevere e gestire e-mail per conto di uno o più domini verificati di tua proprietà.

Disponibilità regionale

Amazon SES supporta la ricezione di e-mail nella tua regione?

Amazon SES supporta la ricezione di e-mail solo in determinate regioni AWS. Per l'elenco completo delle regioni in cui è supportata la ricezione di e-mail, consulta Endpoint e quote di Amazon Simple Email Service in Riferimenti generali di AWS.

Client e-mail basati su POP o IMAP

È possibile utilizzare Microsoft Outlook per ricevere messaggi di posta elettronica in arrivo?

Amazon SES non include i server POP o IMAP per la ricezione di e-mail in entrata. Ciò significa che non è possibile utilizzare un client e-mail Microsoft Outlook per ricevere e-mail in entrata. Se desideri una soluzione in grado di inviare e ricevere e-mail utilizzando un client e-mail, ti consigliamo di utilizzare Amazon WorkMail.

Utilizzo di altri servizi AWS

Hai configurato le autorizzazioni appropriate?

Se desideri che la tua posta venga consegnata in un bucket S3, pubblicata in un argomento Amazon SNS che non è di tua proprietà, attivare una funzione Lambda oppure utilizzare una chiave master personalizzata, dovrai concedere ad Amazon SES l'autorizzazione per accedere a tali risorse. Per

fornire l'accesso ad Amazon SES, devi creare le opportune policy sulle risorse dalle console o dall'API dei relativi servizi AWS. Per ulteriori informazioni, consulta Concessione di autorizzazioni.

Contenuto delle e-mail

Come vuoi che Amazon SES ti passi il contenuto delle e-mail?

Amazon SES può fornire il contenuto delle e-mail in due modi: può archiviare le e-mail in un bucket S3 specificato da te oppure inviarti una notifica Amazon SNS che contenga una copia del messaggio e-mail. Amazon SES consegna l'e-mail in formato raw non modificato Multipurpose Internet Mail Extensions (MIME). Per ulteriori informazioni sul formato MIME, consulta RFC 2045.

Quali dimensioni hanno le email che riceverai?

Se archivi le e-mail in un bucket S3, il limite massimo di dimensione delle e-mail (incluse le intestazioni) è di 40 MB. Se ricevi le e-mail tramite notifiche Amazon SNS, il limite massimo di dimensione delle e-mail (incluse le intestazioni) è 150 KB.

Come vuoi attivare l'elaborazione della tua posta?

Dopo la consegna, vorrai elaborare la posta usando il tuo codice. Ad esempio, la tua applicazione può convertire le e-mail codificate in base 64 in un formato visualizzabile, quindi renderle disponibili a un utente finale attraverso un client e-mail. Puoi avviare il processo in due modi:

- Se le e-mail vengono consegnate ad Amazon S3, la tua applicazione può rimanere in ascolto delle notifiche Amazon SNS generate dalle operazioni S3, estrarre quindi l'ID messaggio dell'e-mail dalle notifiche e utilizzarlo per recuperare l'e-mail da Amazon S3.

  Alternativamente, puoi integrare l'elaborazione delle e-mail nelle regole di ricezione scrivendo una funzione Lambda. In questo caso, la regola di ricezione deve prima scrivere l'e-mail in Amazon S3 e, successivamente, attivare la funzione Lambda. Le operazioni Lambda possono essere eseguite in modo sincrono o asincrono dall'interno delle regole di ricezione, a seconda che la funzione Lambda debba restituire o meno un risultato che influenzi il modo in cui le altre operazioni vengono eseguite. Consigliamo di utilizzare l'esecuzione asincrona, a meno che la sincrona sia assolutamente necessaria nel tuo caso d'uso. Per ulteriori informazioni su AWS Lambda, consulta la Guida per sviluppatori di AWS Lambda.
- Se le e-mail vengono consegnate attraverso una notifica Amazon SNS utilizzando l'operazione SNS, la tua applicazione può rimanere in ascolto delle notifiche Amazon SNS, quindi estrarre i messaggi e-mail dalle notifiche.

Desideri che le e-mail siano crittografate?

Amazon SES si integra con AWS Key Management Service (AWS KMS) per crittografare opzionalmente la posta che scrive nel tuo bucket S3. Amazon SES utilizza la crittografia lato client per crittografare la posta prima di scriverla in Amazon S3. Questo significa che devi decrittare i contenuti sul tuo lato dopo aver recuperato la posta da Amazon S3. AWS SDK for Java e AWS SDK for Ruby forniscono un client che può gestire la decriptazione per te. Amazon SES può crittografare le e-mail solo per te se scegli che vengano consegnate in un bucket S3.

Posta indesiderata

A che punto del processo di ricezione di e-mail desideri bloccare la posta indesiderata?

Quando un mittente cerca di inviare un'e-mail a un destinatario, il server e-mail del mittente scambia una sequenza di comandi con il server del destinatario. Questa sequenza è chiamata conversazione SMTP.

Puoi bloccare e-mail in entrata in due punti del processo di ricezione e-mail: durante la conversazione SMTP e dopo la conversazione SMTP. Utilizza i filtri degli indirizzi IP per bloccare i messaggi durante la conversazione SMTP e le regole di ricezione per bloccare messaggi e-mail dopo la conversazione SMTP.

Puoi utilizzare filtri degli indirizzi IP per bloccare e-mail provenienti da indirizzi IP specifici. Il vantaggio dell'utilizzo dei filtri degli indirizzi IP per bloccare la posta indesiderata è che i messaggi bloccati durante la conversazione SMTP non vengono addebitati. Lo svantaggio dell'utilizzo dei filtri degli indirizzi IP è che rifiutano e-mail da indirizzi IP specificati senza eseguire alcuna analisi sul contenuto effettivo dei messaggi. Per ulteriori informazioni sui filtri degli indirizzi IP, consulta Spiegazione passo per passo per la creazione dei filtri per indirizzi IP tramite la console.

Puoi utilizzare regole di ricezione per inviare una notifica di mancato recapito al mittente di un'e-mail in base all'indirizzo (o dominio o sottodominio) cui il messaggio è stato inviato. Il vantaggio dell'utilizzo di regole di ricezione è che puoi eseguire analisi aggiuntiva su messaggi in entrata prima di inviare una notifica di mancato recapito al mittente. Ad esempio, puoi usare AWS Lambda per inviare notifiche di mancato recapito solo quando i messaggi non superano l'autenticazione DKIM o vengono identificati come spam. Lo svantaggio dell'utilizzo di regole di ricezione è che, poiché vengono elaborate dopo la conversazione SMTP, verrà addebitato un costo per ogni messaggio ricevuto. È anche possibile che ti venga addebitato un costo se utilizzi Lambda per analizzare il contenuto dei messaggi in entrata. Per ulteriori informazioni sulle regole di ricezione, consulta Spiegazione passo per passo sulla console delle regole di ricezione. Per ulteriori informazioni sull'utilizzo di Lambda per analizzare le e-mail in arrivo, consulta Esempi di funzione Lambda.

Flussi di posta

Come desideri dividere il tuo flusso di posta?

Molto probabilmente il tuo dominio riceve diverse classi di posta. Ad esempio, alcuni messaggi del tuo dominio, come un'e-mail a user@example.com, potrebbero essere destinati a una cartella di posta in arrivo personale. Altri messaggi, ad esempio un'e-mail a unsubscribe@example.com, potrebbero essere meglio indirizzati a sistemi automatizzati. Puoi utilizzare le regole di ricezione per dividere le tue e-mail in entrata in modo che possano essere elaborate in modo diverso. Per informazioni su come configurare le regole di ricezione, consulta Creazione delle regole di ricezione.

Autenticazione della ricezione di e-mail e scansione malware

Amazon SES autentica ogni e-mail ricevuta e, facoltativamente, ne analizza il contenuto alla ricerca di spam e malware. SES non intraprende alcuna operazione sull'e-mail ricevuta in base ai risultati dell'autenticazione dell'e-mail o della scansione del contenuto; tuttavia, i risultati di queste operazioni vengono forniti come attributi che è possibile utilizzare nelle operazioni delle regole di ricezione SES, come ad esempio notifiche Amazon SNS o come intestazioni in un messaggio consegnato ad Amazon S3.

Autenticazione dell'e-mail

Amazon SES autentica ogni e-mail ricevuta utilizzando SPF, DKIM e DMARC. I risultati di ciascun meccanismo di autenticazione sono forniti nelle notifiche Amazon SNS inviate da SES nell'ambito della valutazione delle regole nel set di regole di ricezione attivo. Inoltre, se hai scelto di ricevere una copia dell'e-mail in Amazon S3, il risultato dell'autenticazione dell'e-mail viene acquisito nell'intestazione `Authentication-Results` che SES aggiunge alla sezione di intestazione dell'e-mail:

```
Authentication-Results: example.com;
spf=pass (spfCheck: 10.0.0.1 is permitted by domain of example.com) client-ip=10.0.0.1;
 envelope-from=example@example.com; helo=10.0.0.1;
dkim=pass header.i=example.com;
dkim=permerror header.i=some-example.com;
dmarc=pass header.from=example@example.com;
```

L'intestazione `Authentication-Results` è descritta in RFC 8601

Scansione del contenuto delle e-mail per il rilevamento di spam e malware

Amazon SES analizza il contenuto delle e-mail ricevute alla ricerca di malware in base al valore dell'attributo ScanEnabled (API) o Spam and virus scanning (Scansione di spam e virus) (console) della regola di ricezione corrispondente all'e-mail. Per impostazione predefinita, SES analizza il contenuto delle e-mail ricevute alla ricerca di malware. Per disabilitare la scansione del contenuto per le e-mail ricevute che corrispondono a una specifica regola di ricezione, devi impostare il flag della regola di ricezione ScanEnabled su falso se utilizzi l'API o deselezionare la casella di controllo Spam and virus scanning (Scansione di spam e virus) se utilizzi la console. Se per la regola di ricezione corrispondente a un'e-mail è attivata la scansione, il risultato della scansione del contenuto viene fornito nelle notifiche Amazon SNS inviate da SES nell'ambito della valutazione delle regole nel set di regole di ricezione attivo. Inoltre, se hai scelto di ricevere una copia dell'e-mail in Amazon S3, il risultato della scansione del contenuto viene acquisito nelle intestazioni `X-SES-Spam-Verdict` e `X-SES-Virus-Verdict` che SES aggiunge alla sezione di intestazione dell'e-mail.

```
X-SES-Spam-Verdict: PASS
X-SES-Virus-Verdict: FAIL
```

I valori possibili per le intestazioni di cui sopra sono elencati in:

- spam
- virus

Ora che hai compreso i concetti di ricezione dell'e-mail, del funzionamento e dei casi d'uso, puoi iniziare con Configurazione della ricezione di e-mail.

Configurazione della ricezione di e-mail in Amazon SES

In questa sezione vengono descritti i prerequisiti necessari prima di iniziare a configurare Amazon SES per ricevere la posta. È importante che tu abbia letto Concetti di ricezione e-mail e casi d'uso per comprendere i concetti su come funziona Amazon SES e per considerare il modo in cui desideri ricevere, filtrare ed elaborare la tua posta elettronica.

Prima di configurare la ricezione della posta elettronica creando un set di regole, regole di ricezione e filtri per indirizzi IP, devi completare per prima cosa i seguenti prerequisiti di configurazione:

- Verifica il dominio con Amazon SES pubblicando record DNS per provare che è di tua proprietà.
- Consenti ad Amazon SES di ricevere e-mail per il tuo dominio pubblicando un record MX.

- Concedi ad Amazon SES l'autorizzazione ad accedere ad AWS per eseguire le operazioni delle regole di ricezione.

Quando crei e verifichi un'identità di dominio, pubblichi i record nelle impostazioni DNS per completare il processo di verifica, ma solo questo non è sufficiente per utilizzare la ricezione della posta elettronica. Per la ricezione di e-mail, è anche necessario pubblicare un record MX per specificare un dominio MAIL FROM personalizzato. Questo record viene utilizzato nelle impostazioni DNS del dominio per consentire a SES di ricevere e-mail per il dominio. L'assegnazione delle autorizzazioni è necessaria perché le operazioni scelte nelle regole di ricezione non funzioneranno, a meno che Amazon SES non disponga dell'autorizzazione a utilizzare il rispettivo servizio AWS necessario per tali operazioni.

Questi tre prerequisiti necessari per utilizzare la ricezione della posta elettronica sono descritti negli argomenti seguenti:

- Verifica del dominio per la ricezione di e-mail con Amazon SES
- Pubblicazione di un registro MX per la ricezione di e-mail Amazon SES
- Concessione di autorizzazioni ad Amazon SES per la ricezione di e-mail

Verifica del dominio per la ricezione di e-mail con Amazon SES

Come per qualsiasi dominio che intendi utilizzare per l'invio o la ricezione di e-mail con Amazon SES, è innanzitutto necessario provare che è di tua proprietà. La procedura di verifica comprende l'avvio della verifica del dominio con Amazon SES e la successiva pubblicazione dei registri DNS sotto forma di CNAME o TXT nel provider DNS, a seconda del metodo di verifica utilizzato.

Tramite la console, puoi verificare i tuoi domini con Easy DKIM o Bring Your Own DKIM (BYODKIM) e copiare facilmente i rispettivi registri DNS per la pubblicazione nel tuo provider DNS. Per farlo, consulta la spiegazione nella sezione Creazione di un'identità dominio. Facoltativamente, puoi utilizzare le API `VerifyDomainDkim` o `VerifyDomainIdentity` di SES.

Puoi facilmente confermare che il tuo dominio o indirizzo e-mail sia stato verificato facendo riferimento al relativo stato nella tabella Verified Identities (Identità verificate) nella console SES oppure tramite le API `GetIdentityVerificationAttributes` o `GetEmailIdentity` di SES.

Pubblicazione di un registro MX per la ricezione di e-mail Amazon SES

Un record Mail Exchanger (record MX) è una configurazione che specifica quali server di posta possono accettare e-mail inviate al tuo dominio.

Perché Amazon SES possa gestire le e-mail in entrata, occorre aggiungere un registro MX alla configurazione DNS del dominio. Il registro MX creato fa riferimento all'endpoint che riceve e-mail della Regione AWS in cui utilizzi Amazon SES. Ad esempio, l'endpoint della Regione Stati Uniti occidentali (Oregon) è xinbound-smtp.us-west-2.amazonaws.com.x Per un elenco completo degli endpoint, consulta Regioni ed endpoint Amazon SES.

> **Note**
>
> L'endpoint che riceve e-mail in Amazon SES non sono server e-mail IMAP o POP3. Non puoi utilizzare questi URL come server di posta in arrivo nel client e-mail.
> Se desideri una soluzione in grado di inviare e ricevere e-mail utilizzando un client e-mail, ti consigliamo di utilizzare Amazon WorkMail.

La procedura seguente include le fasi generali per la creazione di un record MX. Le procedure specifiche per la creazione di un record MX dipendono dal provider di hosting o DNS. Consulta la documentazione del provider per informazioni sull'aggiunta di un record MX alla configurazione DNS del tuo dominio.

> **Note**
>
> Per completare la procedura seguente, è necessario essere in grado di modificare i record DNS per il dominio. Se non sei in grado di accedere ai registri DNS per il dominio o se l'operazione non è agevole, contatta l'amministratore di sistema per ricevere assistenza.

Aggiunta di un registro MX alla configurazione DNS per il dominio

1. Accedi alla console di gestione del provider DNS.
2. Crea un nuovo registro MX.
3. Per Name (Nome) del registro MX, inserisci il dominio. Ad esempio, se Amazon SES deve gestire e-mail inviate al dominio esempio.com, immetti quanto segue:

```
example.com
```

> **Note**
>
> Alcuni provider DNS chiamano il campo Name (Nome) come Host, Domain (Dominio) o Mail Domain (Dominio di posta).

4. Per Type (Tipo), scegli MX.

> **Note**
>
> Alcuni provider DNS chiamano il campo Type (Tipo) come Record Type (Tipo di record) o un nome simile.

5. In Value (Valore), immetti quanto segue:

```
10 inbound-smtp.region.amazonaws.com
```

Nell'esempio precedente, sostituisci *`Regione`* con l'indirizzo dell'endpoint che riceve e-mail per la Regione AWS utilizzata con Amazon SES. Ad esempio se utilizzi la Regione US East (Virginia settentrionale), sostituisci *`region`* con `us-east-1`. Per un elenco completo degli endpoint di ricezione e-mail , consulta Regioni ed endpoint Amazon SES.

> **Note**
>
> Le console di gestione di alcuni provider DNS includono campi separati per il record Value (Valore) e il record Priority (Priorità). Se questo è il caso per il provider DNS, immetti `10` per il valore Priority (Priorità) e immetti l'URL dell'endpoint e-mail in entrata per Value (Valore).

Istruzioni per la creazione di record MX per diversi provider

Le procedure per la creazione di un record MX per il dominio dipendono dal provider DNS utilizzato. Questa sezione include i collegamenti alla documentazione di diversi provider DNS. Non si tratta di un elenco esaustivo dei provider. Con ogni probabilità, puoi utilizzare la documentazione con Amazon

SES anche se il provider non è indicato nell'elenco. L'inclusione in questo elenco non costituisce una raccomandazione né l'approvazione di alcun prodotto o servizio di alcuna azienda.

Nome del provider di DNS/hosting	Collegamento alla documentazione
Amazon Route 53	Creazione di registro utilizzando la console Amazon Route 53
GoDaddy	Aggiunta di un record MX (collegamento esterno)
DreamHost	Come posso modificare i miei record MX? (collegamento esterno)
Cloudflare	Configurazione dei record di e-mail (collegamento esterno)
HostGator	Modifica dei record MX - Windows (collegamento esterno)
Namecheap	Come posso configurare i record MX richiesti per il servizio di posta? (collegamento esterno)
Names.co.uk	Modifica delle impostazioni DNS del dominio (collegamento esterno)
Wix	Aggiunta o aggiornamento di record MX nell'account Wix (collegamento esterno)

Concessione di autorizzazioni ad Amazon SES per la ricezione di e-mail

Alcune delle attività che puoi eseguire quando ricevi e-mail in Amazon SES, ad esempio l'invio di e-mail a un bucket Amazon Simple Storage Service (Amazon S3) o la chiamata ad una funzione AWS Lambda, richiedono autorizzazioni speciali. Questa sezione include gli esempi di policy per diversi casi d'uso comuni.

Argomenti in questa sezione:

- Concessione ad Amazon SES dell'autorizzazione per la scrittura su un bucket S3

- Concessione ad Amazon SES l'autorizzazione a utilizzare la tua chiave AWS KMS
- Concessione ad Amazon SES dell'autorizzazione a richiamare la funzione AWS Lambda
- Concessione ad Amazon SES dell'autorizzazione alla pubblicazione in un argomento Amazon SNS appartenente a un account AWS diverso

Concessione ad Amazon SES dell'autorizzazione per la scrittura su un bucket S3

Se applicata a un bucket S3, la seguente policy concede ad Amazon SES l'autorizzazione a scrivere nel bucket specificato. Per ulteriori informazioni sulla creazione di regole di ricezione per il trasferimento di e-mail in entrata ad Amazon S3, consulta Operazione di consegna a bucket S3.

Per maggiori informazioni sulle politiche dei bucket S3, consulta Utilizzo delle policy dei bucket e dell'utente nella Guida per l'utente di 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"
        }
      }
    }
  ]
}
```

Nel precedente esempio di policy, apporta le modifiche seguenti:

- Sostituisci *myBucket* con il nome del bucket S3 in cui desideri scrivere.
- Sostituisci *region* con la regione AWS in cui hai creato la regola di ricezione.

- Sostituisci *111122223333* con l'ID del tuo account AWS.
- Sostituisci *rule_set_name* con il nome del set di regole che contiene la regola di ricezione contenente l'operazione di consegna al bucket di Amazon S3.
- Sostituisci *nome_rule_recept_* con il nome della regola di ricezione che contiene l'operazione di spedizione al bucket Amazon S3.

Concessione ad Amazon SES l'autorizzazione a utilizzare la tua chiave AWS KMS

Per poter crittografare le tue e-mail, Amazon SES deve disporre dell'autorizzazione a utilizzare la chiave AWS KMS che hai specificato durante la configurazione delle regole di ricezione. Puoi utilizzare la chiave di default KMS (aws/ses) nel tuo account o una chiave personalizzata creata da te. Se utilizzi la chiave di default KMS, non devi eseguire nessuna procedura per concedere ad Amazon SES l'autorizzazione a utilizzarla. Se utilizzi una chiave personalizzata, devi concedere ad Amazon SES l'autorizzazione a utilizzarla aggiungendo un'istruzione alla policy della chiave.

Utilizza la seguente informativa sulla policy come criterio chiave per consentire ad Amazon SES di utilizzare la chiave personalizzata per permettere al cliente di ricevere e-mail sul tuo 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"
        }
      }
}
```

Nel precedente esempio di policy, apporta le modifiche seguenti:

- Sostituisci *region* con la regione AWS in cui hai creato la regola di ricezione.

- Sostituisci *111122223333* con l'ID del tuo account AWS.
- Sostituisci *rule_set_name* con il nome del set di regolamenti che contiene la regola di ricezione associata alla ricezione e-mail.
- Sostituisci *nome_rule_recept_* con il nome della regola di ricezione associata alla ricezione e-mail.

Se usi AWS KMS per inviare messaggi crittografati a un bucket S3 con crittografia lato server abilitata, è necessario aggiungere l'azione dei criteri, `"kms:Decrypt"`. Utilizzando l'esempio precedente, l'aggiunta di questa azione al criterio apparirà come segue:

```
{
  "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"
        }
      }
}
```

Per ulteriori informazioni su come allegare policy a chiavi AWS KMS, consulta Utilizzo delle policy chiave in AWS KMS nella Guida per sviluppatori di AWS Key Management Service.

Concessione ad Amazon SES dell'autorizzazione a richiamare la funzione AWS Lambda

Per abilitare la richiesta di una funzione AWS Lambda da parte di Amazon SES, puoi scegliere la funzione quando crei una regola di ricezione nella console di Amazon SES. Quando lo fai, Amazon SES aggiunge automaticamente le autorizzazioni necessarie alla funzione.

In alternativa, puoi usare l'operazione `AddPermission` nell'API AWS Lambda per collegare una policy a una funzione. La seguente chiamata all'API `AddPermission` concede ad Amazon SES l'autorizzazione di chiamare la funzione Lambda. Per ulteriori informazioni su come allegare policy a funzioni Lambda, consulta Autorizzazioni AWS Lambdanella Guida per gli sviluppatori di 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"
}
```

Nel precedente esempio di policy, apporta le modifiche seguenti:

- Sostituisci *region* con la regione AWS in cui hai creato la regola di ricezione.
- Sostituisci *111122223333* con l'ID del tuo account AWS.
- Sostituisci *rule_set_name* con il nome del set di regole contenenti la regola di ricezione dove è stata creata la funzione Lambda.
- Sostituisci *recepit_rule_name* con il nome della regola di ricezione contenente la funzione Lambda.

Concessione ad Amazon SES dell'autorizzazione alla pubblicazione in un argomento Amazon SNS appartenente a un account AWS diverso

Per pubblicare notifiche in un argomento di un account AWS separato, devi allegare una policy all'argomento Amazon SNS. L'argomento SNS deve trovarsi nella stessa regione del dominio e del set di regole di ricezione.

La policy seguente concede ad Amazon SES l'autorizzazione a pubblicare in un argomento Amazon SNS in un account AWS separato.

```
{
  "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"
        }
      }
    }
  ]
}
```

Nel precedente esempio di policy, apporta le modifiche seguenti:

- Sostituisci *topic_region* con l'Regione AWS in cui l'argomento Amazon SNS è stato creato.
- Sostituisci *sns_topic_account_id* con l'ID dell'account AWS proprietario dell'argomento Amazon SNS.
- Sostituisci *topic_name* con il nome dell'argomento Amazon SNS in cui desideri pubblicare le notifiche.
- Sostituisci *aws_account_id* con l'ID dell'account AWS configurato per ricevere e-mail.
- Sostituisci *receipt_region* con l'Regione AWS in cui è stata creata la regola di ricezione.
- Sostituisci *rule_set_name* con il nome del set di regole che contiene la regola di ricezione in cui è stata creata l'operazione di pubblicazione di Amazon SNS.
- Sostituisci *receipt_rule_name* con il nome della regola di ricezione contenente l'operazione dell'argomento di pubblicazione su Amazon SNS.

Se l'argomento Amazon SNS utilizza AWS KMS per la crittografia lato server, devi aggiungere autorizzazioni alla policy delle chiavi AWS KMS. Puoi aggiungere autorizzazioni collegando la policy seguente alla policy delle chiavi AWS KMS:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
```

```
            "Sid": "AllowSESToUseKMSKey",
            "Effect": "Allow",
            "Principal": {
                "Service": "ses.amazonaws.com"
            },
            "Action": [
                "kms:GenerateDataKey",
                "kms:Decrypt"
            ],
            "Resource": "*"
        }
    ]
}
```

Spiegazioni passo per passo sulla console di ricezione e-mail di Amazon SES

In questa sezione vengono descritte le procedure guidate della console di ricezione della posta elettronica utilizzate per la configurazione di regole di ricezione e filtri per indirizzi IP per gestire la ricezione della posta elettronica. Prima di utilizzare le procedure guidate della console, è importante aver letto Concetti di ricezione e-mail e casi d'uso per capire i concetti sul funzionamento della ricezione di e-mail e Configurazione della ricezione di e-mailper assicurarti di aver eseguito i prerequisiti di configurazione.

Le procedure guidate della console per la configurazione delle regole di ricezione e dei filtri degli indirizzi IP sono illustrate di seguito:

- Spiegazione passo per passo sulla console delle regole di ricezione
- Spiegazione passo per passo per la creazione dei filtri per indirizzi IP tramite la console

Spiegazione passo per passo sulla console delle regole di ricezione

Questa sezione illustra la creazione e la definizione delle regole di ricezione utilizzando la console Amazon SES. I punti chiave per capire come funzionano le regole di ricezione sono:

- set di regole, che contengono una serie ordinata di regole di ricezione, e regole di ricezione, che contengono un insieme ordinato di operazioni.
- Le regole di ricezione indicano ad Amazon SES come gestire la posta in arrivo eseguendo un elenco ordinato di operazioni specificate.

- Questo elenco ordinato di azioni facoltativamente può essere reso dipendente dalla prima corrispondenza di una condizione del destinatario; se non specificato, le operazioni verranno applicate a tutte le identità che appartengono ai tuoi domini verificati.
- Le regole di ricezione vengono create e definite in un container denominato come set di regole; sebbene sia possibile creare più set di regole, è possibile averne solo uno attivo alla volta.
- Le regole di ricezione all'interno del set di regole attivo vengono eseguite nell'ordine specificato.
- Per creare regole di ricezione, per prima cosa è necessario creare un set di regole per contenerle.

In alternativa, puoi usare l'API `CreateReceiptRuleSet` per creare un set di regole di ricezione vuoto, come descritto nella Documentazione di riferimento per le API di Amazon Simple Email Service. In seguito, puoi usare la console Amazon SES o l'API `CreateReceiptRule` per aggiungervi regole di ricezione.

Prima di procedere con la spiegazione passo per passo, assicurati di aver soddisfatto tutti i prerequisiti necessari per utilizzare la ricezione di e-mail basata sul destinatario. Inoltre

Prerequisiti

È necessario soddisfare i seguenti prerequisiti prima di procedere con l'impostazione del controllo e-mail in base ai destinatari utilizzando regole di ricezione:

1. Assicurati che il tuo endpoint si trovi in una Regione AWS per la quale Amazon SES supporta la ricezione di e-mail. Consulta la sezione SES supported email receiving endpoints (Endpoint supportati da SES per la ricezione di e-mail).
2. Per prima cosa devi creare e verificare un'identità del dominio in Amazon SES.
3. Successivamente, devi specificare quali server di posta possono accettare la posta per il dominio pubblicando un record MX nelle impostazioni DNS del dominio. (Il record MX creato deve far riferimento all'endpoint Amazon SES che riceve e-mail della Regione AWS in cui utilizzi Amazon SES).
4. Infine, concedi ad Amazon SES l'autorizzazione ad accedere ad altre risorse AWS per eseguire le operazioni delle regole di ricezione.

Creazione di set di regole e regole di ricezione

Questa spiegazione passo per passo inizia creando innanzitutto un set di regole che contenga le regole e procede con la procedura guidata Create rule (Crea regola) per creare, definire e ordinare

le regole di ricezione. La procedura guidata contiene quattro schermate per definire le impostazioni delle regole, aggiungere le condizioni dei destinatari, aggiungere operazioni e rivedere tutte le impostazioni.

Creazione di una regola di ricezione tramite la console

1. Accedi alla AWS Management Console e apri la console Amazon SES all'indirizzo https://console.aws.amazon.com/ses/.
2. Nel pannello di navigazione di sinistra, in Email Receiving (Ricezione e-mail), scegli Rule Sets (Set di regole).

   > **Note**
   >
   > Ricezione di e-mail non sarà visibile nel riquadro di navigazione a sinistra della console SES se l'account si trova in una Regione AWS in cui SES non supporta la ricezione di e-mail. Esamina la prima voce elencata in the section called “Prerequisiti”.

3. Nella scheda Set di regole di ricezione nel riquadro Ricezione di e-mail, scegli Crea set di regole.
4. Immetti un nome univoco per il set di regole e scegli Create rule set (Crea set di regole).
5. Scegli Create rule (Crea una regola) per aprire la procedura guidata per Create rule (Crea una regola).
6. Alla pagina Define rule settings (Definisci impostazioni della regola), in Receipt rule details (Dettagli regola di ricezione), immetti un nome per Rule name (Nome regola).
7. Per Status (Stato), deseleziona solo la casella Enabled (Abilitato) se non vuoi che Amazon SES esegua questa regola dopo la creazione; in caso contrario, lascia selezionata questa opzione.
8. (Opzionale) In Security and protection options (Opzioni di sicurezza e protezione), per Transport Layer Security (TLS), seleziona Required (Obbligatorio) se desideri che Amazon SES rifiuti i messaggi in arrivo che non vengono inviati tramite una connessione sicura.
9. (Opzionale) Se vuoi che Amazon SES analizzi le e-mail in arrivo in cerca di spam e virus, per Spam and virus scanning (Scansione di spam e virus), seleziona Enabled (Abilitata).
10. Scegli Next (Successivo) per procedere.
11. (Opzionale) Nella pagina Add recipient conditions (Aggiungi condizioni destinatario), utilizza la procedura seguente per specificare una o più condizioni del destinatario. Puoi definire un massimo di 100 condizioni del destinatario per ogni regola di ricezione.

a. In Recipient conditions (Condizioni del destinatario), scegli Add new recipient condition (Aggiungi nuova condizione del destinatario) per specificare l'indirizzo e-mail di ricezione o il dominio a cui si desidera applicare la regola di ricezione. La tabella seguente usa l'indirizzo utente@esempio.com per mostrare come specificare i destinatari.

Se vuoi...	Specifica il destinatario seguente...	Note
Specificare come corrispondente un determinato indirizzo e-mail.	utente@esempio.com	Include anche le corrispondenze con le varianti dell'indirizzo che contengono etichette, ad esempio utente+123@esempio.com e utente+xyz@esempio.com. Tuttavia, se specifichi un indirizzo che contiene un'etichetta, verrà considerato come corrispondente solo l'indirizzo specifico.
Specificare come corrispondenti tutti gli indirizzi all'interno di un dominio, ma non quelli all'interno del sottodominio.	esempio.com	
Specificare come corrispondenti tutti gli indirizzi all'interno di un sottodominio specifico, ma non quelli all'interno del dominio padre.	sottodominio.esempio.com	

Se vuoi...	Specifica il destinatario seguente...	Note
Specificare come corrispondenti tutti gli indirizzi all'interno di tutti i sottodomini, ma non quelli all'interno del dominio padre.	.esempio.com	Nota il punto (.) prima del nome di dominio.
Specificare come corrispondenti tutti gli indirizzi all'interno di un dominio e all'interno di tutti i sottodomini.	esempio.com .esempio.com	Crea due destinatari separati: uno con il nome di dominio e uno con un punto seguito dal nome di dominio.
Specificare come corrispondenti tutti i destinatari in tutti i domini verificati	[Nessuno]	Lascia vuoto il campo del destinatario.

> **Important**
>
> Se più account Amazon SES ricevono e-mail in un dominio comune, ad esempio se più team nella stessa azienda hanno account Amazon SES separati, Amazon SES elabora simultaneamente tutte le regole di ricezione corrispondenti per ognuno degli account. Questo comportamento può produrre una situazione in cui un account genera un mancato recapito, mentre un altro accetta l'e-mail.
> Ti consigliamo di coordinarti con gli altri team dell'organizzazione che usano Amazon SES per fare in modo che ogni account usi regole di ricezione univoche e che queste regole non si sovrappongano. In questi casi, è preferibile configurare le regole di ricezione in modo da usare solo gli indirizzi e-mail o i sottodomini univoci per il gruppo o il team.

b. Ripeti questo passaggio per ogni condizione del destinatario che desideri aggiungere. Dopo aver aggiunto le condizioni del destinatario, scegli Next (Successivo).

12. Usa la procedura seguente per aggiungere una o più operazioni alla regola di ricezione nella pagina Add actions (Aggiungi operazioni).

    a. Apri il menu Add new action (Aggiungi nuova operazione), quindi scegli uno dei seguenti tipi di operazioni:

    - Aggiunta di intestazioni: questa operazione aggiunge un'intestazione personalizzata alle e-mail ricevute.
    - Risposta di mancato recapito o ritorno: questa operazione rifiuta l'e-mail ricevuta restituendo una risposta di mancata recapito al mittente.
    - Chiamata di una funzione Lambda: questa operazione chiama il codice tramite una funzione AWS Lambda.
    - Consegna a bucket S3: questa operazione archivia l'e-mail ricevuta in un bucket Amazon Simple Storage Service (S3).
    - Pubblicazione in un argomento Amazon SNS: questa operazione pubblica l'e-mail completa in un argomento Amazon Simple Notification Service (SNS).
    - Interruzione del set di regole: questa operazione arresta la valutazione del set di regole di ricezione.
    - Integrazione con Amazon WorkMail: questa operazione si integra con Amazon WorkMail.

    Per ulteriori informazioni su tutte queste operazioni, consulta Opzioni per le operazioni.

    b. Ripeti questo passaggio per ogni operazione da definire. Se sono state definite più operazioni, è possibile riordinarle utilizzando le frecce verso l'alto e verso il basso all'interno dei container di operazioni. Scegli Next (Successivo), per aprire la pagina Review (Rivedi).

13. Nella pagina Review (Rivedi), riesamina le impostazioni e le operazioni della regola. Se hai necessità di apportare modifiche, scegli l'opzione Edit (Modifica) o utilizza la sezione di navigazione a sinistra nella pagina per passare direttamente alla pagina con il contenuto da modificare. In alternativa, puoi apportare modifiche all'ordine delle operazioni elencate nella tabella Actions (Operazioni) della pagina Review (Rivedi) utilizzando le frecce verso l'alto e verso il basso nella colonna Reorder (Riordina).
14. Quando sei pronto per continuare, seleziona Create user (Crea utente).
15. Nella pagina di conferma del set di regole, scegli Imposta come attivo se desideri applicare immediatamente il set di regole.

Modifica delle regole dopo la creazione

Dopo aver creato un set di regole, è possibile modificare sia il set di regole che le regole di ricezione in esso contenute. Oltre a modificarle, è anche possibile duplicare il set di regole o le relative regole, in modo da crearne rapidamente di nuove. Nell'elenco riportato di seguito vengono illustrate le modifiche disponibili per il set di regole e le regole di ricezione:

- L'elenco per Rule set (Set di regole) comprende il nome, lo stato e la data di creazione. Le opzioni di modifica per il set di regole sono:
  - Set as active/inactive (Imposta come attivo/inattivo), che permette di passare tra le impostazioni dello stato.
  - Duplicate (Duplica), che permette di copiare il set di regole. Verrà richiesto di specificare un nome univoco.
  - Delete (Elimina), che permette di eliminare il set di regole. Verrà richiesto di confermare questa operazione irreversibile.
- Receipt rules (Regole di ricezione), che sono elencate con nome, stato, sicurezza e ordine. Le opzioni di modifica per le regole di ricezione sono:
  - Up/down arrows (Frecce verso l'alto/verso il basso) per riordinare l'esecuzione delle regole all'interno del set di regole.
  - Duplicate (Duplica), che permette di creare una copia della regola selezionata. Verrà richiesto di specificare un nome univoco.
  - Il pulsante Edit (Modifica) aprirà la regola selezionata in modo che sia possibile modificare qualsiasi parametro, ad esempio le impostazioni delle regole, le condizioni del destinatario e le operazioni.
  - Il pulsante Delete (Elimina) eliminerà la regola selezionata. Verrà richiesto di confermare questa operazione irreversibile.
  - Il pulsante Create rule (Crea regola) ti permetterà di creare una nuova regola al set di regole corrente.

Opzioni per le operazioni

Ogni regola di ricezione per il ricevimento di e-mail su Amazon SES contiene un elenco ordinato di operazioni. Questa sezione descrive le opzioni specifiche per ogni tipo di operazione.

I tipi di operazione sono i seguenti:

- Operazione di aggiunta intestazioni
- Operazione di risposta mancato recapito o ritorno
- Chiamata di un'operazione della funzione Lambda
- Operazione di consegna a bucket S3
- Operazione di pubblicazione in un argomento Amazon SNS
- Operazione di interruzione del set di regole
- Operazione di integrazione con Amazon WorkMail

Operazione di aggiunta intestazioni

L'operazione Add Header (Aggiungi intestazione) aggiunge un'intestazione personalizzata alle e-mail ricevute. In genere, questa operazione viene usata solo in combinazione con un'altra. Questa operazione include le opzioni seguenti.

- Header name (Nome intestazione): nominativo da aggiungere all'intestazione. Deve contenere da 1 a 50 caratteri inclusi e solo caratteri alfanumerici (a-z, A-Z, 0-9) e trattini.
- Header value (Valore intestazione): valore da aggiungere all'intestazione. Deve contenere meno di 2048 caratteri e non può includere caratteri di nuova riga ("\r" o"\n").

Operazione di risposta mancato recapito o ritorno

L'operazione Bounce (Mancato recapito) rifiuta l'e-mail restituendo una risposta di mancato recapito al mittente e, facoltativamente, ti invia una notifica tramite Amazon SNS. Questa operazione include le opzioni seguenti.

- SMTP Reply Code (Codice di risposta SMTP): codice di risposta SMTP, in base a quanto definito dallo standard RFC 5321.
- SMTP Status Code (Codice di stato SMTP): codice di stato avanzato SMTP, in base a quanto definito dallo standard RFC 3463.
- Message (Messaggio): testo leggibile da includere nell'e-mail di mancato recapito.
- Reply Sender (Mittente per risposta): l'indirizzo e-mail del mittente la cui e-mail che non è stata recapitata. Si tratta dell'indirizzo da cui è stata inviata l'e-mail di mancato recapito. Deve essere verificato con Amazon SES.
- SNS Topic (Argomento SNS): nome o ARN dell'argomento Amazon SNS cui inviare facoltativamente una notifica quando viene inviata un'e-mail di mancato recapito. Un esempio

di ARN di un argomento Amazon SNS è arn:aws:sns:us-east-1:123456789012:MyTopic. Puoi anche creare un argomento Amazon SNS quando configuri l'operazione scegliendo Create SNS Topic (Crea argomento SNS). Per ulteriori informazioni su Amazon SNS, consulta la Guida per gli sviluppatori di Amazon Simple Notification Service.

> **Note**
>
> L'argomento Amazon SNS scelto deve trovarsi nella stessa Regione AWS dell'endpoint Amazon SES usato come ricevitore delle e-mail.

Puoi digitare valori personalizzati per questi campi oppure puoi scegliere un modello che completi automaticamente i campi SMTP Reply Code (Codice di risposta SMTP), SMTP Status Code (Codice di stato SMTP) e Message (Messaggio) con valori basati sul motivo del mancato recapito. Sono disponibili i seguenti modelli:

- Mailbox Does Not Exist (La mailbox non esiste): SMTP Reply Code (Codice di risposta SMTP) = 550, SMTP Status Code (Codice di stato SMTP) = 5.1.1
- Message Too Large (Messaggio troppo grande): SMTP Reply Code (Codice di risposta SMTP) = 552, SMTP Status Code (Codice di stato SMTP) = 5.3.4
- Mailbox Full (Casella di posta piena): SMTP Reply Code (Codice di risposta SMTP) = 552, SMTP Status Code (Codice di stato SMTP) = 5.2.2
- Message Content Rejected (Contenuto messaggio rifiutato): SMTP Reply Code (Codice di risposta SMTP) = 500, SMTP Status Code (Codice di stato SMTP) = 5.6.1
- Unknown Failure (Errore sconosciuto): SMTP Reply Code (Codice di risposta SMTP) = 554, SMTP Status Code (Codice di stato SMTP) = 5.0.0
- Temporary Failure (Errore temporaneo): SMTP Reply Code (Codice di risposta SMTP) = 450, SMTP Status Code (Codice di stato SMTP) = 4.0.0

Per informazioni su altri codici di mancato recapito che puoi usare digitando valori personalizzati nei campi, consulta RFC 3463.

Chiamata di un'operazione della funzione Lambda

L'operazione Lambda chiama il codice tramite una funzione e, eventualmente, invia una notifica tramite Amazon SNS. Questa operazione della regola presenta le seguenti opzioni e requisiti.

Opzioni

- Lambda function (Funzione Lambda): l'ARN della funzione Lambda. Un esempio di ARN di una funzione Lambda è arn:aws:lambda:us-east-1:account-id:function:MyFunction.
- Invocation type (Tipo di chiamata): tipo di chiamata della funzione Lambda. Un tipo di invocazione di RequestResponse significa che l'esecuzione della funzione si traduce in una risposta immediata. Un tipo di invocazione di Event (Evento) significa che la funzione viene richiamata in modo asincrono. Ti consigliamo di usare il tipo di chiamata Event (Evento), a meno che l'esecuzione sincrona non sia assolutamente necessaria per il tuo caso d'uso.

  Nelle chiamate RequestResponse si verifica un time-out dopo 30 secondi.

  Per ulteriori informazioni, consulta Richiamo di funzioni AWS Lambda nella Guida per gli sviluppatori di AWS Lambda.
- SNS Topic (Argomento SNS): nome o ARN dell'argomento Amazon SNS cui inviare una notifica quando viene attivata la funzione Lambda specificata. Un esempio di ARN di un argomento Amazon SNS è arn:aws:sns:us-east-1:123456789012:MyTopic. Per le istruzioni, consulta Creazione di un argomento Amazon SNS nella Guida per lo Sviluppatore di Amazon Simple Notification Service.

Requisiti

- La funzione Lambda che scegli deve trovarsi nella stessa regione AWS dell'endpoint Amazon SES che usi per ricevere e-mail.
- L'argomento Amazon SNS che scegli deve trovarsi nella stessa regione AWS dell'endpoint Amazon SES che usi per ricevere e-mail.

Scrittura della funzione Lambda

Per elaborare l'e-mail, la funzione Lambda può essere richiamata in modo asincrono, ovvero usando il tipo di chiamata `Event`. L'eventuale oggetto passato alla funzione Lambda conterrà i metadati relativi all'evento di e-mail in arrivo. Puoi usare i metadati anche per accedere al contenuto del messaggio dal bucket Amazon S3.

Se vuoi controllare effettivamente il flusso di posta, la funzione Lambda deve essere richiamata in modo sincrono, ovvero usando il tipo di chiamata `RequestResponse` e la funzione Lambda deve chiamare il metodo `callback` con due argomenti: il primo argomento è `null` e il secondo

argomento è una proprietà `disposition` impostata su `STOP_RULE`, `STOP_RULE_SET` o `CONTINUE`. Se il secondo argomento è `null` o non ha una proprietà `disposition` valida, il flusso di posta continua e vengono elaborate ulteriori operazioni e regole. Questo comportamento corrisponde all'uso del valore `CONTINUE`.

Ad esempio, puoi arrestare la regola di ricezione impostata scrivendo la riga di codice seguente alla fine del codice della funzione Lambda:

```
callback( null, { "disposition" : "STOP_RULE_SET" });
```

Per alcuni esempi di codice AWS Lambda, consulta Esempi di funzione Lambda. Per alcuni esempi di casi d'uso generali, consulta Esempi di casi d'uso.

Formato di input

Amazon SES passa informazioni alla funzione Lambda in formato JSON. L'oggetto di primo livello contiene una matrice `Records`, che viene popolata con le proprietà `eventSource`, `eventVersion` e `ses`. L'oggetto `ses` contiene oggetti `receipt` e `mail`, che hanno esattamente lo stesso formato delle notifiche Amazon SNS; descritte in Contenuti delle notifiche.

I dati che Amazon SES trasmette a Lambda includono metadati relativi al messaggio, oltre a diverse intestazioni di posta elettronica. Tuttavia, non contiene il corpo del messaggio.

Di seguito viene mostrata una vista generale della struttura dell'input fornito da Amazon SES per la funzione Lambda.

```
{
   "Records": [
      {
        "eventSource": "aws:ses",
        "eventVersion": "1.0",
        "ses": {
           "receipt": {
               <same contents as SNS notification>
            },
           "mail": {
               <same contents as SNS notification>
           }
         }
     }
   ]
```

```
}
```

Valori restituiti

La funzione Lambda può controllare il flusso di posta restituendo uno dei valori seguenti:

- `STOP_RULE`: non verranno elaborate ulteriori operazioni nella regola di ricezione corrente, ma possono essere elaborate altre regole di ricezione.
- `STOP_RULE_SET`: non verranno elaborate ulteriori operazioni o regole di ricezione.
- `CONTINUE` o qualsiasi altro valore non valido: indica che è possibile elaborare ulteriori operazioni e regole di ricezione.

Negli argomenti seguenti vengono illustrati alcuni esempi di eventi di posta in arrivo, esempi di casi d'uso generali ed esempi di codice AWS Lambda:

- Esempi di casi d'uso
- Esempi di funzione Lambda

Esempi di casi d'uso

Gli esempi seguenti mostrano alcune regole che puoi configurare per usare i risultati della funzione Lambda in modo da controllare il flusso di posta. Per scopi dimostrativi, molti di questi esempi usano l'operazione S3 come risultato.

Caso d'uso 1: eliminazione della spam in tutti i domini

Questo esempio mostra una regola globale che elimina la spam in tutti i domini. Le regole 2 e 3 sono incluse per mostrare che puoi applicare regole specifiche del dominio dopo l'eliminazione dello spam in tutti i domini.

Regola 1

Elenco di destinatari: vuoto. Di conseguenza, questa regola si applica a tutti i destinatari in tutti i domini verificati.

Operazioni

1. Operazione Lambda (sincrona) che restituisce `STOP_RULE_SET` se l'e-mail è spam. In caso contrario, restituisce `CONTINUE`. Consulta la funzione Lambda come esempio per l'eliminazione di spam in Esempi di funzione Lambda.

Regola 2

Elenco di destinatari: esempio1.com

Operazioni

1. Qualsiasi operazione.

Regola 3

Elenco di destinatari: esempio2.com

Operazioni

1. Qualsiasi operazione.

Caso d'uso 2: mancato recapito di spam in tutti i domini

Questo esempio mostra una regola globale che specifica il mancato recapito dello spam in tutti i domini. Le regole 2 e 3 sono incluse per mostrare che puoi applicare regole specifiche del dominio dopo il mancato recapito della spam in tutti i domini.

Regola 1

Elenco di destinatari: vuoto. Di conseguenza, questa regola si applica a tutti i destinatari in tutti i domini verificati.

Operazioni

1. Operazione Lambda (sincrona) che restituisce `CONTINUE` se l'e-mail è spam. In caso contrario, restituisce `STOP_RULE`.
2. Operazione di mancato recapito ("500 5.6.1. Message content rejected" (500 5.6.1 Contenuto messaggio rifiutato)).
3. Operazione Stop (Interrompi).

Regola 2

Elenco di destinatari: esempio1.com

Operazioni

1. Qualsiasi operazione

Regola 3

Elenco di destinatari: esempio2.com

Operazioni

1. Qualsiasi operazione

Caso d'uso 3: applicazione della regole più specifica

Questo esempio mostra come usare l'operazione di interruzione per impedire l'elaborazione delle e-mail tramite più regole. In questo esempio, supponi di aver definito una regola per un indirizzo specifico e un'altra per tutti gli indirizzi e-mail nel dominio. Usando l'operazione di interruzione, i messaggi che corrispondono alla regola per l'indirizzo e-mail specifico non vengono elaborati dalla regola più generica applicata al dominio.

Regola 1

Elenco di destinatari: user@example.com

Operazioni

1. Operazione Lambda (asincrona).
2. Operazione Stop (Interrompi).

Regola 2

Elenco di destinatari: example.com

Operazioni

1. Qualsiasi operazione.

Caso d'uso 4: registro degli eventi di posta elettronica su CloudWatch

Questo esempio mostra come mantenere un registro di verifica di tutta la posta trasmessa nel sistema prima di salvare la posta in Amazon SES.

Regola 1

Elenco di destinatari: example.com

Operazioni

1. Operazione Lambda (asincrona) che scrive l'oggetto evento in un registro CloudWatch. L'esempio Lambda funziona nel registro Esempi di funzione Lambda in CloudWatch.
2. Operazione S3.

Caso d'uso 5: eliminazione di posta che non supera la convalida DKIM

Questo esempio mostra come salvare tutte le e-mail in arrivo in un bucket Amazon S3 inviando solo le e-mail destinate a un indirizzo e-mail specifico e che superano la convalida DKIM nella tua applicazione di e-mail automatica.

Regola 1

Elenco di destinatari: example.com

Operazioni

1. Operazione S3.
2. Operazione Lambda (sincrona) che restituisce `STOP_RULE_SET` se il messaggio non supera la convalida DKIM. In caso contrario, restituisce `CONTINUE`.

Regola 2

Elenco di destinatari: support@example.com

Operazioni

1. Operazione Lambda (asincrona) che attiva l'applicazione automatica.

Caso d'uso 6: esclusione della posta in base all'oggetto

Questo esempio mostra come eliminare tutta la posta in arrivo di un dominio che contiene la parola "discount" nell'oggetto, quindi elaborare la posta destinata a un sistema automatico in un modo, elaborando invece la posta indirizzata a tutti gli altri destinatari nel dominio in un modo diverso.

Regola 1

Elenco di destinatari: example.com

Operazioni

1. Operazione Lambda (sincrona) che restituisce `STOP_RULE_SET` se l'oggetto contiene la parola "discount". In caso contrario, restituisce `CONTINUE`.

Regola 2

Elenco di destinatari: support@example.com

Operazioni

1. Operazione S3 con bucket 1.
2. Operazione Lambda (asincrona) che attiva l'applicazione automatica.
3. Operazione Stop (Interrompi).

Regola 3

Elenco di destinatari: example.com

Operazioni

1. Operazione S3 con bucket 2.
2. Operazione Lambda (asincrona) che elabora l'e-mail per il resto del dominio.

Esempi di funzione Lambda

Questo argomento contiene alcuni esempi di funzioni Lambda che controllano il flusso di posta.

Esempio 1: eliminazione della spam

Questo esempio interrompe l'elaborazione dei messaggi che includono almeno un indicatore di 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);
    }
};
```

Esempio 2: continua se viene trovata una particolare intestazione

Questo esempio continua a elaborare la regola corrente solo se l'e-mail contiene un valore di intestazione specifico.

```
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'});
};
```

Esempio 3: recupero dell'e-mail da Amazon S3

Questo esempio ottiene l'e-mail in formato RAW da Amazon S3 e la elabora.

> **Note**
>
> Devi prima scrivere l'e-mail in Amazon S3 usando un'operazione 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);
            }
        });
};
```

Esempio 4: mancato recapito dei messaggi per i quali l'autenticazione DMARC ha avuto esito negativo

Questo esempio invia un messaggio di mancato recapito se l'autenticazione DMARC di un'e-mail in arrivo ha esito negativo.

> **Note**
>
> Quando usi questo esempio, imposta il valore della variabile di ambiente `emailDomain` sul dominio di ricezione delle e-mail.

```
'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();
    }
};
```

Operazione di consegna a bucket S3

L'operazione S3 recapita l'e-mail in un bucket Amazon S3 e, facoltativamente, ti invia una notifica tramite Amazon SNS. Questa operazione include le opzioni seguenti.

- S3 Bucket (Bucket S3): nome del bucket Amazon S3 nel quale salvare le e-mail ricevute. Puoi anche creare un nuovo bucket Amazon S3 quando configuri l'operazione scegliendo Create S3

Bucket (Crea bucket S3). Amazon SES fornisce l'e-mail non modificata e in formato RAW, che è in genere in formato Multipurpose Internet Mail Extensions (MIME). Per ulteriori informazioni sul formato MIME, consulta RFC 2045.

> **Important**
>
> - Quando salvi le e-mail in un bucket Simple Storage Service (Amazon S3), la dimensione massima di default per le e-mail (incluse le intestazioni) è di 40 MB.
> - SES non supporta le regole di ricezione che caricano nei bucket S3 abilitati con il blocco oggetti configurato e un periodo di conservazione di default.
> - Se applichi la crittografia ai bucket S3 mediante la tua chiave KMS, assicurati di utilizzare l'ARN della chiave KMS completamente qualificata e non l'alias della chiave KMS; l'utilizzo dell'alias potrebbe comportare la crittografia dei dati con una chiave KMS che appartiene al richiedente e non all'amministratore del bucket. Consulta la sezione Utilizzo della crittografia per operazioni tra più account.
> - SES non supporta i bucket S3 nelle regioni Opt-in come destinazione per le e-mail in entrata.

- Object Key Prefix (Prefisso oggetto chiave): prefisso del nome della chiave da usare nel bucket Amazon S3. I prefissi dei nomi della chiave permettono di organizzare il bucket Amazon S3 in una struttura di cartelle. Ad esempio, se usi Email come Object Key Prefix (Prefisso oggetto chiave), le e-mail appariranno nel bucket Amazon S3 in una cartella denominata Email.
- KMS Key (Chiave KMS) (se è selezionato "Encrypt Message" (Crittografa messaggio) nella console Amazon SES): la chiave AWS KMS che deve essere usata da Amazon SES per crittografare le e-mail prima di salvarle nel bucket Amazon S3. Puoi usare la chiave KMS di default o una chiave gestita del cliente creata in AWS KMS.

> **Note**
>
> La chiave KMS scelta deve trovarsi nella stessa Regione AWS dell'endpoint Amazon SES usato per ricevere e-mail.

  - Per usare la chiave KMS di default predefinita, scegli aws/ses quando configuri la regola di ricezione nella console Amazon SES. Se usi un API Amazon SES, puoi fornire la chiave KMS di default specificando un ARN nel formato `arn:aws:kms:REGION:AWSACCOUNTID:alias/`

`aws/ses`. Ad esempio, se il tuo ID account AWS è 123456789012 e vuoi usare la chiave KMS di default nella regione us-east-1, l'ARN della chiave KMS di default sarà `arn:aws:kms:us-east-1:123456789012:alias/aws/ses`. Se usi la chiave KMS di default, non devi completare altre fasi per concedere ad Amazon SES l'autorizzazione necessaria per usare la chiave.

- Per usare una chiave gestita del cliente creata in AWS KMS, specifica l'ARN della chiave KMS e assicurati di aggiungere un'istruzione alla policy della chiave per concedere ad Amazon SES l'autorizzazione necessaria per usarla. Per ulteriori informazioni su come concedere autorizzazioni, consulta Concessione di autorizzazioni ad Amazon SES per la ricezione di e-mail.

Per ulteriori informazioni sull'utilizzo di AWS KMS con Amazon SES, consulta la Guida per sviluppatori di AWS Key Management Service. Se non specifichi una chiave KMS nella console o nell'API, Amazon SES non potrà crittografare le e-mail.

> **Important**
>
> La posta viene crittografata da Amazon SES tramite il client di crittografia Amazon S3 prima che la posta venga inviata ad Amazon S3 per l'archiviazione. Non viene crittografata tramite la crittografia lato server di Amazon S3. Questo significa che devi usare il client di crittografia Amazon S3 per decrittare l'e-mail dopo averla recuperata da Amazon S3, perché il servizio non ha l'accesso per usare le tue chiavi AWS KMS per la decrittazione. Questo client di crittografia è disponibile in AWS SDK for Java e in AWS SDK for Ruby. Per maggiori informazioni, consulta la Guida per l'utente di Amazon Simple Storage Service.

- SNS Topic (Argomento SNS): nome o ARN dell'argomento Amazon SNS cui inviare una notifica quando l'e-mail viene salvata nel bucket Amazon S3. Un esempio di ARN di un argomento Amazon SNS è arn:aws:sns:us-east-1:123456789012:MyTopic. Puoi anche creare un argomento Amazon SNS quando configuri l'operazione scegliendo Create SNS Topic (Crea argomento SNS). Per ulteriori informazioni su Amazon SNS, consulta la Guida per gli sviluppatori di Amazon Simple Notification Service.

> **Note**
>
> L'argomento Amazon SNS scelto deve trovarsi nella stessa Regione AWS dell'endpoint Amazon SES usato come ricevitore delle e-mail.

Operazione di pubblicazione in un argomento Amazon SNS

L'operazione SNS pubblica la posta usando una notifica Amazon SNS. La notifica include il contenuto completo dell'e-mail. Questa operazione include le opzioni seguenti.

- SNS Topic (Argomento SNS): nome o ARN dell'argomento Amazon SNS in cui pubblicare le e-mail. Le notifiche Amazon SNS includeranno una copia non modificata e in formato RAW dell'e-mail, in genere in formato Multipurpose Internet Mail Extensions (MIME). Per ulteriori informazioni sul formato MIME, consulta RFC 2045.

  > **Important**
  >
  > Se scegli di ricevere le e-mail tramite notifiche Amazon SNS, il limite massimo di dimensione delle e-mail (incluse le intestazioni) è 150 KB. Le e-mail di dimensioni maggiori non vengono recapitate. Se prevedi e-mail con dimensioni maggiori di questo limite, salvale invece in un bucket Amazon S3.

  Un esempio di ARN di un argomento Amazon SNS è arn:aws:sns:us-east-1:123456789012:MyTopic. Puoi anche creare un argomento Amazon SNS quando configuri l'operazione scegliendo Create SNS Topic (Crea argomento SNS). Per ulteriori informazioni su Amazon SNS, consulta la Guida per gli sviluppatori di Amazon Simple Notification Service.

  > **Note**
  >
  > L'argomento Amazon SNS scelto deve trovarsi nella stessa Regione AWS dell'endpoint Amazon SES usato come ricevitore delle e-mail.

- Encoding (Codifica): codifica da usare per l'e-mail all'interno della notifica Amazon SNS. La codifica UTF-8 è più facile da usare, ma potrebbe non conservare tutti i caratteri speciali se un messaggio è stato codificato con un formato di codifica diverso. La codifica Base64 conserva tutti i caratteri speciali. Per informazioni su UTF-8 e Base64, consulta rispettivamente RFC 3629 e RFC 4648.

Quando ricevi una e-mail, Amazon SES esegue le regole contenute nel set di regole di ricezione attivo. Puoi configurare le regole di ricezione per inviare notifiche tramite Amazon SNS. Le regole di ricezione possono inviare due diversi tipi di notifiche:

- Notifiche inviate da operazioni SNS: quando aggiungi un'operazione SNS a una regola di ricezione, invia informazioni sull'e-mail, incluso il suo contenuto. Se il messaggio è pari o minore di 150 KB, questo tipo di notifica include anche il corpo MIME completo dell'e-mail.
- Notifiche inviate da altri tipi di operazioni: quando aggiungi qualsiasi altro tipo di operazione (tra cui le operazioni Bounce (Mancato recapito), Lambda, Stop Rule Set (Set di regole di interruzione) o WorkMail) a una regola di ricezione, è facoltativo specificare un argomento Amazon SNS. Specificando l'argomento, riceverai notifiche quando queste operazioni vengono eseguite. Queste operazioni contengono informazioni sull'e-mail, ma non contengono il contenuto dell'e-mail.

Questa sezione descrive i contenuti delle notifiche, oltre a fornire un esempio per ciascun tipo di notifica.

- Contenuti delle notifiche per la ricezione di e-mail Amazon SES
- Esempi di notifiche per la ricezione di e-mail di Amazon SES

Contenuti delle notifiche per la ricezione di e-mail Amazon SES

Tutte le notifiche per la ricezione di e-mail vengono pubblicate negli argomenti Amazon Simple Notification Service (Amazon SNS) in formato JSON (JavaScript Object Notation).

Per degli esempi di notifiche, consulta Esempi di notifiche.

Indice

Oggetto JSON di primo livello

L'oggetto JSON di primo livello contiene i campi seguenti.

Nome campo	Descrizione
`notificationType`	Tipo di notifica. Per questo tipo di notifica, il valore è sempre `Received`.
`receipt`	Oggetto che contiene informazioni sulla consegna dell'e-mail.
`mail`	Oggetto che contiene informazioni sull'e-mail a cui la notifica è associata.
`content`	Stringa che contiene l'e-mail in formato RAW non modificato, in genere il formato Multipurp ose Internet Mail Extensions (MIME). Per ulteriori informazioni sul formato MIME, consulta RFC 2045. **Note** Questo campo è presente solo se la notifica è stata attivata da un'operaz ione SNS. Le notifiche attivate da tutte le altre operazioni non contengono questo campo.

Oggetto receipt

L'oggetto `receipt` dispone dei campi seguenti.

Nome campo	Descrizione
`action`	Oggetto che incapsula informazioni sull'oper azione eseguita. Per un elenco di possibili valori, consulta Oggetto action.
`dkimVerdict`	Oggetto che indica se il controllo DomainKey s Identified Mail (DKIM) è stato superato. Per un elenco di possibili valori, consulta Oggetto dkimVerdict.
`dmarcPolicy`	Indica le impostazioni Domain-based Message Authentication, Reporting & Conformance (DMARC) per il dominio di invio. Il campo appare solo se il messaggio fallisce l'autenti cazione DMARC. I valori possibili per questo campo sono: • `none`: il proprietario del dominio di invio richiede che non vengano eseguite operazion i specifiche sui messaggi che non superano l'autenticazione DMARC. • `quarantine` : il proprietario del dominio di invio richiede che i messaggi che non superano l'autenticazione DMARC vengano considerati sospetti dai ricevitori. • `reject`: il proprietario del dominio di invio richiede che i messaggi che non superano l'autenticazione DMARC vengano rifiutati.
`dmarcVerdict`	Oggetto che indica se il controllo DMARC (Domain-based Message Authentication, Reporting & Conformance) è stato superato. Per un elenco di possibili valori, consulta Oggetto dmarcVerdict.

Nome campo	Descrizione
`processingTimeMillis`	Stringa che specifica il periodo di tempo, in millisecondi, dal momento in cui Amazon SES ha ricevuto il messaggio al momento in cui ha attivato l'operazione.
`recipients`	I destinatari (nello specifico, gli indirizzi envelope RCPT TO) abbinati dalla regola di ricezione attiva. Gli indirizzi elencati qui potrebbero differire da quelli elencati dal campo `destination` in the section called “oggetto mail”.
`spamVerdict`	Oggetto che indica il messaggio come spam. Per un elenco di possibili valori, consulta Oggetto spamVerdict.
`spfVerdict`	Oggetto che indica se il controllo Sender Policy Framework (SPF) è stato superato. Per un elenco di possibili valori, consulta Oggetto spfVerdict.
`timestamp`	Stringa che specifica la data e l'ora in cui l'operazione è stata attivata, in formato ISO 8601.
virusVerdict	Oggetto che indica se il messaggio contiene un virus. Per un elenco di possibili valori, consulta Oggetto virusVerdict.

Oggetto action

L'oggetto `action` dispone dei campi seguenti.

Nome campo	Descrizione
`type`	Stringa che indica il tipo di operazione che è stata eseguita. I valori possibili sono `S3`, `SNS`, `Bounce`, `Lambda`, `Stop` e `WorkMail`.
`topicArn`	Stringa che contiene l'Amazon Resource Name (ARN) dell'argomento Amazon SNS in cui la notifica è stata pubblicata.
`bucketName`	Stringa che contiene il nome del bucket Amazon S3 in cui il messaggio è stato pubblicato. Presente solo per il tipo di operazione S3.
`objectKey`	Stringa che include un nome che identifica in modo univoco l'e-mail nel bucket Amazon S3. Ciò corrisponde a `messageId` in the section called “oggetto mail”. Presente solo per il tipo di operazione S3.
`smtpReplyCode`	Stringa che include il codice di risposta SMTP, come definito dallo standard RFC 5321. Presente solo per il tipo di operazione Bounce.
`statusCode`	Stringa che include il codice di stato avanzato SMTP, come definito dallo standard RFC 3463. Presente solo per il tipo di operazione Bounce.
`message`	Stringa che contiene il testo leggibile da includere nel messaggio di mancato recapito. Presente solo per il tipo di operazione Bounce.
`sender`	Stringa che contiene l'indirizzo e-mail del mittente dell'e-mail che non è stata recapitata. Questo è l'indirizzo da cui il messaggio di mancato recapito è stato inviato. Presente solo per il tipo di operazione Bounce.

Nome campo	Descrizione
`functionArn`	Stringa che contiene l'ARN della funzione Lambda che è stata attivata. Presente solo per il tipo di operazione Lambda.
`invocationType`	Stringa che include il tipo di richiamo della funzione Lambda. I valori possibili sono `RequestResponse` e `Event`. Presente solo per il tipo di operazione Lambda.
`organizationArn`	Stringa che contiene l'ARN dell'organizzazione Amazon WorkMail. Presente solo per il tipo di operazione WorkMail.

Oggetto dkimVerdict

L'oggetto `dkimVerdict` dispone dei campi seguenti.

Nome campo	Descrizione
`status`	Stringa che contiene il risultato DKIM. I valori possibili sono: • `PASS`: il messaggio ha superato l'autenti cazione DKIM. • `FAIL`: il messaggio non ha superato l'autenti cazione DKIM. • `GRAY`: il messaggio non è firmato da DKIM o il dominio di provenienza e il dominio con firma DKIM non corrispondono. • `PROCESSING_FAILED` :A un problema impedisce ad Amazon SES di verificare la firma DKIM. Ad esempio, le query DNS non riescono o l'intestazione della firma DKIM non ha il formato corretto.

Oggetto dmarcVerdict

L'oggetto `dmarcVerdict` dispone dei campi seguenti.

Nome campo	Descrizione
`status`	Stringa che contiene il risultato DMARC. I valori possibili sono: • `PASS`: il messaggio ha superato l'autenticazione DMARC. • `FAIL`: il messaggio non ha superato l'autenticazione DMARC. • `GRAY`: almeno uno tra SPF e DKIM ha superato l'autenticazione, ma il dominio di invio non dispone di una policy DMARC o utilizza la policy `p=none`. • `PROCESSING_FAILED` : un problema impedisce ad Amazon SES di fornire un risultato DMARC.

Oggetto spamVerdict

L'oggetto `spamVerdict` dispone dei campi seguenti.

Nome campo	Descrizione
`status`	Stringa che contiene il risultato della scansione di verifica spam. I valori possibili sono: • `PASS`: la scansione di verifica spam ha determinato che non è probabile che il messaggio contenga spam. • `FAIL`: la scansione di verifica spam ha determinato che è probabile che il messaggio contenga spam.

Nome campo	Descrizione
	• `GRAY`: Amazon SES ha analizzato l'e-mail senza poter determinare con sicurezza se si tratta di spam. • `PROCESSING_FAILED` : Amazon SES non è stato in grado di analizzare l'e-mail. Ad esempio, l'e-mail non è un messaggio MIME valido.

Oggetto spfVerdict

L'oggetto `spfVerdict` dispone dei campi seguenti.

Nome campo	Descrizione
`status`	Stringa che contiene il risultato SPF. I valori possibili sono: • `PASS`: il messaggio ha superato l'autenti cazione SPF. • `FAIL`: il messaggio non ha superato l'autenti cazione SPF. • `GRAY`: il risultato SPF è `none`, `softfail` o `neutral`. • `PROCESSING_FAILED` : un problema impedisce ad Amazon SES di verificare il record SPF. Ad esempio, le query DNS non riescono.

Oggetto virusVerdict

L'oggetto `virusVerdict` dispone dei campi seguenti.

Nome campo	Descrizione
`status`	Stringa che contiene il risultato della scansione di verifica virus. I valori possibili sono: • `PASS`: il messaggio non contiene virus. • `FAIL`: il messaggio contiene virus. • `GRAY`: Amazon SES ha analizzato l'e-mail senza poter determinare con sicurezza se contiene virus. • `PROCESSING_FAILED` : Amazon SES non è in grado di analizzare il contenuto dell'e-ma il. Ad esempio, l'e-mail non è un messaggio MIME valido.

oggetto mail

L'oggetto `mail` dispone dei campi seguenti.

Nome campo	Descrizione
`destination`	Un elenco completo di tutti gli indirizzi dei destinatari (inclusi i destinatari A: e Cc:) tratti dalle intestazioni MIME dell'e-mail in entrata.
`messageId`	Stringa che contiene l'ID univoco assegnato all'e-mail da Amazon SES. Se l'e-mail è stata consegnata ad Amazon S3, l'ID messaggio è anche la chiave dell'oggetto Amazon S3 utilizzata per scrivere il messaggio al tuo bucket Amazon S3.
`source`	Stringa che contiene l'indirizzo e-mail da cui l'email è stata inviata (nello specifico, l'indirizzo MAIL FROM della busta).

Nome campo	Descrizione
`timestamp`	Stringa che contiene data e ora in cui l'e-mail è stata ricevuta, in formato ISO8601.
`headers`	Le intestazioni Amazon SES e le intestazioni personalizzate. Ogni intestazione dispone dei campi seguenti: `name` e `value`.
`commonHeaders`	Le intestazioni comuni a tutte le e-mail. Ogni intestazione dispone dei campi seguenti: `name` e `value`.
`headersTruncated`	Stringa che specifica se le intestazioni sono state troncate nella notifica. Ciò si verifica se le intestazioni hanno dimensione superiore a 10 KB. I valori possibili sono `true` e `false`.

Oggetto commonHeaders

L'oggetto `commonHeaders` può avere i campi indicati nella tabella riportata di seguito. I campi presenti in questo oggetto variano a seconda di quali campi erano presenti nella posta in entrata.

Nome campo	Descrizione
`messageId`	L'ID del messaggio originale.
`date`	La data e l'ora in cui Amazon SES ha ricevuto il messaggio.
`to`	L'intestazione To dell'e-mail.
`cc`	L'intestazione CC dell'e-mail.
`bcc`	L'intestazione BCC dell'e-mail.
`from`	L'intestazione From dell'e-mail.
`sender`	L'intestazione Sender dell'e-mail.

Nome campo	Descrizione
`returnPath`	L'intestazione Return-Path dell'e-mail.
`replyTo`	L'intestazione Reply-To dell'e-mail.
`subject`	L'intestazione Subject dell'e-mail.

Esempi di notifiche per la ricezione di e-mail di Amazon SES

Questa sezione include esempi dei seguenti tipi di notifiche:

- Una notifica inviata a seguito di un'operazione SNS.
- Una notifica inviata a seguito di un altro tipo di operazione (una notifica di avviso).

Notifica di un'operazione SNS

Questa sezione contiene un esempio di una notifica di operazione SNS. A differenza della notifica di avviso mostrata in precedenza, essa include una sezione `content` che contiene l'e-mail, in genere nel 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"
}
```

Notifica di avviso

Questa sezione contiene un esempio di una notifica Amazon SNS che può essere attivata da un'operazione S3. Le notifiche attivate da operazioni Lambda, operazioni di mancato recapito, operazioni di interruzione e operazioni WorkMail sono simili. Anche se la notifica contiene informazioni sull'e-mail, non contiene il contenuto dell'e-mail.

```
{
"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"
}
}
}
```

Operazione di interruzione del set di regole

L'operazione Stop (Interrompi) arresta la valutazione del set di regole di ricezione e, facoltativamente, ti invia una notifica tramite Amazon SNS. Questa operazione include le opzioni seguenti.

- SNS Topic (Argomento SNS): nome o ARN dell'argomento Amazon SNS cui inviare una notifica quando viene eseguita l'operazione di interruzione. Un esempio di ARN di un argomento Amazon SNS è arn:aws:sns:us-east-1:123456789012:MyTopic. Puoi anche creare un argomento Amazon SNS quando configuri l'operazione scegliendo Create SNS Topic (Crea argomento SNS). Per ulteriori informazioni su Amazon SNS, consulta la Guida per gli sviluppatori di Amazon Simple Notification Service.

  > **Note**
  >
  > L'argomento Amazon SNS scelto deve trovarsi nella stessa Regione AWS dell'endpoint Amazon SES usato come ricevitore delle e-mail.

Operazione di integrazione con Amazon WorkMail

L'operazione WorkMail si integra con Amazon WorkMail. Se Amazon WorkMail esegue l'elaborazione completa delle e-mail, in genere non devi usare questa operazione direttamente perché Amazon Workmail si occuperà della configurazione. Questa operazione include le opzioni seguenti.

- Organization ARN (organizzazione ARN): l'ARN dell'organizzazione Amazon Workmail. Gli ARN di organizzazione Amazon WorkMail sono in formato `arn:aws:workmail:`*`region`*`:`*`account_ID`*`:organization/`*`organization_ID`*, dove:

- `region` è la regione in cui utilizzi Amazon SES e Amazon WorkMail. Devi usarli nella stessa regione. Ad esempio, us-east-1.
- `account_ID` è l'ID account AWS. Puoi trovare il tuo ID account AWS nella pagina Account della Console di gestione AWS.
- `organization_ID` è un identificatore univoco generato da Amazon Workmail al momento della creazione di un'organizzazione. Puoi trovare l'organizzazione ID nella console Amazon Workmail nella pagina Organization Settings (Impostazioni organizzazione) nella pagina della tua organizzazione.

Un esempio di ARN completo dell'organizzazione Amazon WorkMail è arn:aws:workmail:us-east-1:123456789012:organization/m-68755160c4cb4e29a2b2f8fb58f359d7. Per informazioni sulle organizzazioni Amazon WorkMail, consulta la Guida per l'amministratore di Amazon WorkMail.

- SNS Topic (Argomento SNS): nome o ARN dell'argomento Amazon SNS cui inviare una notifica quando viene eseguita l'operazione Amazon Workmail. Un esempio di ARN di un argomento Amazon SNS è arn:aws:sns:us-east-1:123456789012:MyTopic. Puoi anche creare un argomento Amazon SNS quando configuri l'operazione scegliendo Create SNS Topic (Crea argomento SNS). Per ulteriori informazioni su Amazon SNS, consulta la Guida per gli sviluppatori di Amazon Simple Notification Service.

> **Note**
>
> L'argomento Amazon SNS scelto deve trovarsi nella stessa Regione AWS dell'endpoint Amazon SES usato come ricevitore delle e-mail.

> **Note**
>
> Amazon SES supporta le azioni WorkMail solo nelle regioni in cui WorkMail è disponibile. Consulta Amazon WorkMail endpoints and quotas (Endpoint e quote di Amazon WorkMail) in Riferimenti generali di AWS.

Spiegazione passo per passo per la creazione dei filtri per indirizzi IP tramite la console

Questa sezione illustra la configurazione dei filtri degli indirizzi IP utilizzando la console Amazon SES. Il filtro degli indirizzi IP consente di fornire un ampio livello di controllo. Questi filtri IP consentono di bloccare o consentire esplicitamente tutti i messaggi provenienti da specifici indirizzi IP o intervalli di indirizzi IP.

In alternativa, puoi usare l'API `CreateReceiptFilter` per creare un filtro di indirizzi IP come descritto nella Documentazione di riferimento per le API di Amazon Simple Email Service.

> **Note**
>
> Se desideri ricevere la posta solo da un elenco limitato di indirizzi IP noti, configura un elenco di indirizzi bloccati contenente `0.0.0.0/0` e un elenco di indirizzi permessi contenente gli indirizzi IP attendibili. Questa configurazione blocca tutti gli indirizzi IP per impostazione predefinita e permette la ricezione di posta solo dagli indirizzi IP specificati in modo esplicito.

Prerequisiti

I seguenti prerequisiti devono essere soddisfatti prima di procedere con l'impostazione del controllo e-mail basato sui destinatari utilizzando i filtri degli indirizzi IP:

1. Per prima cosa devi creare e verificare un'identità del dominio in Amazon SES.
2. Successivamente, devi specificare quali server di posta possono accettare la posta per il dominio pubblicando un record MX nelle impostazioni DNS del dominio. (Il record MX creato deve far riferimento all'endpoint Amazon SES che riceve e-mail della Regione AWS in cui utilizzi Amazon SES).

Creazione filtri degli indirizzi IP

Creazione di un filtro degli indirizzi IP tramite la console

1. Accedere alla AWS Management Console e aprire la console Amazon SES all'indirizzo https://console.aws.amazon.com/ses/.
2. Nel pannello di navigazione di sinistra, scegli Email Receiving (Ricezione e-mail).

3. Seleziona la scheda IP address filters (Filtri indirizzi IP).
4. Scegli Create Filter (Crea filtro).
5. Inserisci un nome univoco per il filtro; la legenda del campo indicherà i requisiti di sintassi. (Il nome deve contenere meno di 64 caratteri alfanumerici, trattini (-), caratteri di sottolineatura (_) e punti (.); deve iniziare e terminare con una lettera e un numero).
6. Immetti un indirizzo IP o un intervallo di indirizzi IP; la legenda del campo fornisce alcuni esempi specificati nella sintassi CIDR (Classless Inter-Domain Routing). Un esempio di indirizzo IP singolo è 10.0.0.1; un esempio di un intervallo di indirizzi IP è 10.0.0.1/24. Per ulteriori informazioni sulla notazione CIDR, consulta RFC 2317.
7. Scegli Policy type (Tipo di policy), selezionando il pulsante Block (Blocca) o Allow (Consenti).
8. Scegli Create Filter (Crea filtro).
9. Se desideri aggiungere un altro filtro IP, scegli Create filter (Crea filtro) e ripeti i passaggi precedenti per ogni filtro aggiuntivo che desideri aggiungere.
10. Se desideri rimuovere un filtro di indirizzi IP, selezionalo insieme alla casella di controllo Delete (Elimina).

Visualizzazione di parametri per la ricezione di e-mail di Amazon SES

Se hai abilitato la ricezione di e-mail in Amazon SES e hai creato regole di ricezione per le tue e-mail, puoi visualizzare i parametri relativi a tali set di regole e regole di ricezione utilizzando Amazon CloudWatch.

Nella CloudWatch console, troverai le metriche in Metriche > Tutte le metriche > SES > Metriche del set di regole di ricezione e Metriche delle regole di ricezione.

> **Note**
>
> Parametri set di regole di ricezione e Parametri regola di ricezione non verranno visualizzate in SES se ancora non è stata:
>
> - abilitata la ricezione di e-mail
> - creata qualsiasi regola di ricezione
> - ricevuta un'e-mail che corrisponde a una qualsiasi delle regole.

Sono disponibili i seguenti parametri dei messaggi:

- Ricezione di messaggi

Ambito	Parametro	Descrizione	Dimensione
Parametri del set di regole di ricezione	Ricevuto	SES ha ricevuto correttamente un messaggio che dispone di almeno una regola valida. Questo parametro può avere solo un valore di 1.	RuleSetName
Parametri delle regole di ricezione	Ricevuto	SES ha ricevuto correttamente un messaggio e tenterà di elaborare la regola applicata. Questo parametro può avere solo un valore di 1.	RuleName

- Pubblicazione di messaggi

Ambito	Parametro	Descrizione	Dimensione
Parametri del set di regole di ricezione	PublishSuccess	SES ha eseguito correttamente tutte le regole che si applicano all'interno di un set di regole.	RuleSetName
Parametri delle regole di ricezione	PublishSuccess	SES ha eseguito correttamente una regola che si applica al messaggio in arrivo.	RuleName
Parametri del set di regole di ricezione	PublishFailure	SES ha riscontrato un errore durante il tentativo di eseguire le regole all'interno di un set di regole, l'esecuzione verrà ritentata.	RuleSetName
Parametri delle regole di ricezione	PublishFailure	SES ha riscontrato un errore durante il tentativo di eseguire le azioni in una regola: a seconda dell'errore, è possibile che venga eseguito un nuovo tentativo di esecuzione.	RuleName

Ambito	Parametro	Descrizione	Dimensione
Parametri del set di regole di ricezione	PublishExpired	SES non tenterà più di eseguire le regole perché non hanno avuto successo entro 36 ore o hanno riscontrato un errore non recuperabile.	RuleSetName
Parametri delle regole di ricezione	PublishExpired	SES non tenterà più di eseguire le azioni della regola perché non hanno avuto successo entro 36 ore.	RuleName

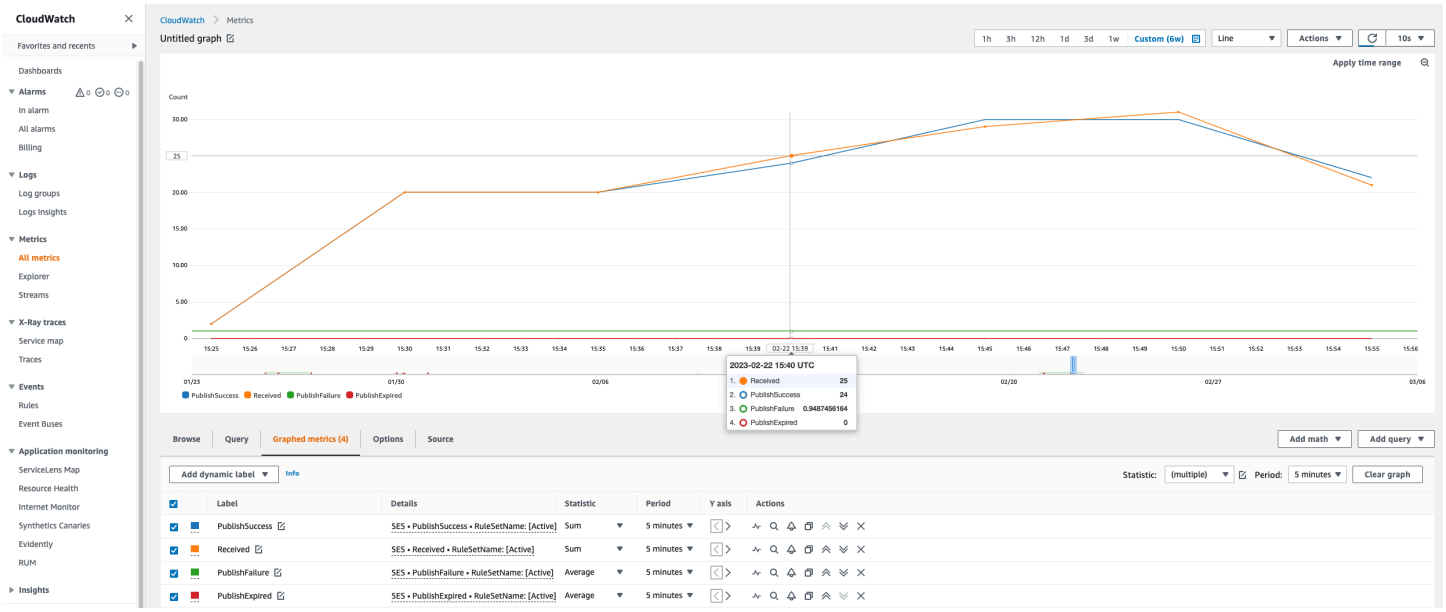
Note

- Nelle tabelle precedenti, il termine si applica indica che il mittente non è negli elenchi di blocco dei filtri IP o è nell'elenco di blocco interno di SES e che la regola dispone di condizioni del destinatario corrispondenti e policy TLS corrispondente.
- Errori di mancata pubblicazione possono verificarsi, ad esempio, se sono state eliminate o revocate le autorizzazioni per un bucket Amazon S3, un argomento Amazon SNS o una funzione Lambda per il cui utilizzo è stata configurata un'operazione in una delle regole di ricezione.
- Poiché può essere attivo solo un set di regole alla volta, SES pubblica una metrica aggregata visualizzata come RuleSetName: [Attivo] per tutti i set di regole che erano attivi nell'intervallo di tempo selezionato. CloudWatch In questo modo è possibile modificare liberamente i set di regole senza alcuna modifica alla configurazione degli allarmi.

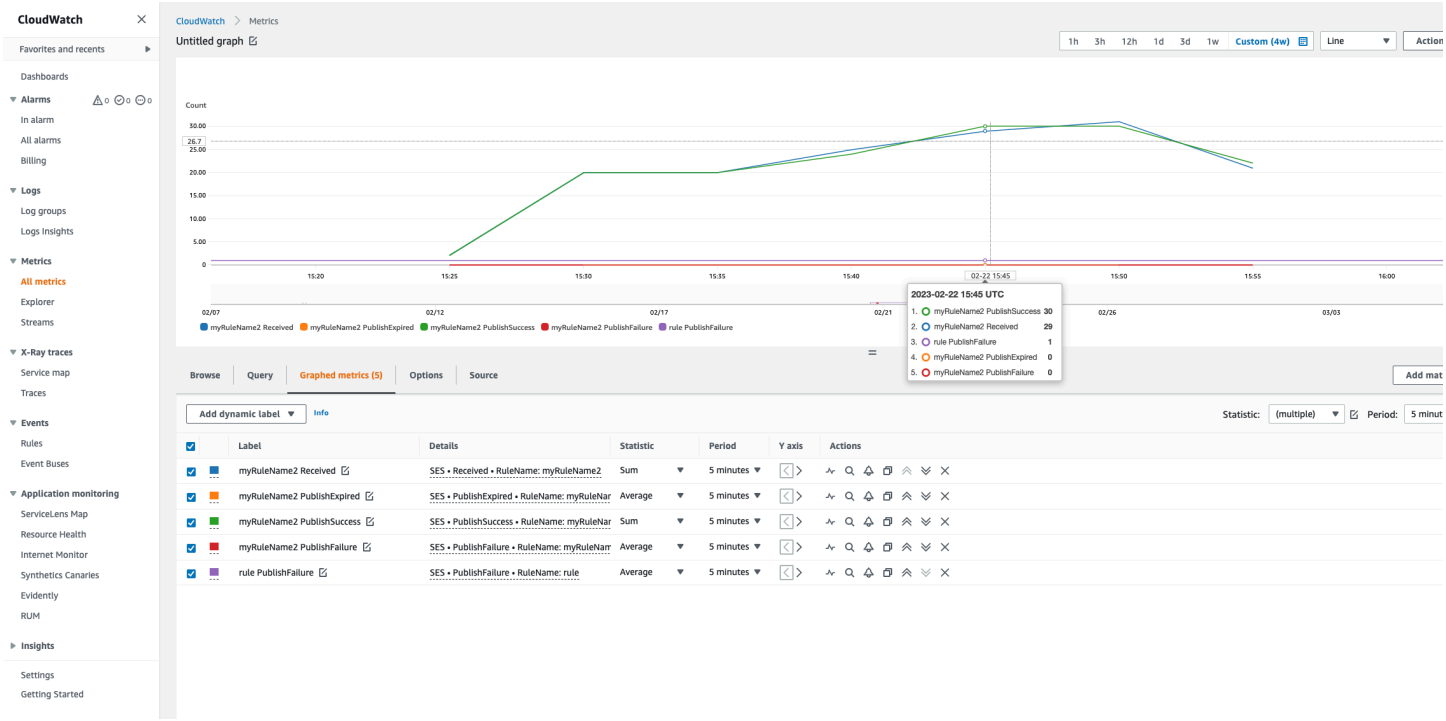
Important

Le modifiche apportate per correggere il set di regole di ricezione saranno applicate solo alle e-mail ricevute da Amazon SES dopo l'aggiornamento. I messaggi e-mail vengono sempre valutati rispetto al set di regole di ricezione applicato quando il messaggio è stato ricevuto.

Metriche per un set di regole di ricezione SES visualizzate nella console. CloudWatch



Metriche per una regola di ricezione SES visualizzate nella CloudWatch console.



Identità verificate in Amazon SES

In Amazon SES, un'identità verificata è un dominio o un indirizzo e-mail che puoi utilizzare per inviare e-mail. Prima di poter inviare un'e-mail utilizzando Amazon SES, devi verificare ogni identità che desideri utilizzare come indirizzo "From" (Da), "Source" (Origine), "Sender" (Mittente) o "Return-Path" (Percorso di ritorno) per provare che sia di tua proprietà. Verificando un'identità con Amazon SES, confermi di esserne il proprietario e impedisce l'utilizzo non autorizzato.

Se il tuo account si trova ancora nella sandbox Amazon SES, devi inoltre verificare tutti gli indirizzi e-mail a cui intendi inviare e-mail, tranne gli indirizzi e-mail di test forniti dal simulatore di mailbox Amazon SES. Per ulteriori informazioni, consulta the section called “Utilizzo manuale del simulatore di mailbox”.

Puoi verificare un'identità utilizzando la console Amazon SES oppure l'API Amazon SES. Il processo di verifica dell'identità dipende dal tipo di identità che si sceglie di creare.

> **Tip**
>
> Se utilizzi SES per la prima volta, puoi utilizzare la procedura guidata introduttiva per creare e verificare la tua prima identità (indirizzo e-mail o dominio).

Indice

Creazione e verifica delle identità in Amazon SES

In Amazon SES, puoi creare un'identità a livello di dominio oppure creare identità di indirizzi e-mail. Questi tipi di identità non si escludono a vicenda. Nella maggior parte dei casi, la creazione di un'identità di dominio elimina la necessità di creare e verificare identità di singoli indirizzi e-mail, a meno che non desideri applicare configurazioni personalizzate a un indirizzo di posta elettronica specifico. Puoi sia creare un dominio e utilizzare indirizzi e-mail basati sul dominio, sia creare singoli

indirizzi e-mail; entrambi gli approcci hanno dei vantaggi. Il metodo scelto dipende dalle tue esigenze specifiche come discusso di seguito.

La creazione e la verifica dell'identità di un indirizzo e-mail è il modo più rapido per iniziare a usare SES, ma la verifica di un'identità a livello di dominio comporta diversi vantaggi. Una volta verificata un'identità di dominio, puoi inviare e-mail solo da quell'indirizzo e-mail ma quando verifichi un'identità di dominio, potrai inviare e-mail da qualsiasi sottodominio o indirizzo e-mail del dominio verificato senza verificare singolarmente ciascuno di essi. Ad esempio, se crei e verifichi un'identità di dominio denominata example.com, non avrai bisogno di creare identità separate per i sottodomini a.example.com, a.b.example.com né per le identità di indirizzi e-mail separati, come user@example.com, user@a.example.com e così via.

Tuttavia, tieni presente che l'identità di un indirizzo e-mail che utilizza la verifica ereditata dal suo dominio è limitata al semplice invio di e-mail. Se vuoi un invio avanzato, dovrai verificarla esplicitamente anche come identità di un indirizzo e-mail. L'invio avanzato include l'utilizzo dell'indirizzo e-mail con set di configurazione, autorizzazioni di policy per l'invio delegato e configurazioni che sovrascrivono le impostazioni del dominio.

Per chiarire l'ereditarietà di verifica e le funzionalità di invio e-mail discusse sopra, la tabella seguente classifica ogni combinazione di verifica dominio/indirizzo e-mail ed elenca l'ereditarietà, il livello di invio e lo stato di visualizzazione per ciascuna di esse:

	Solo dominio verificato	Solo indirizzo e-mail verificato	Sia il dominio che l'indirizzo e-mail verificati
Livello di ereditarietà	I sottodomini e gli indirizzi e-mail ereditano la verifica dal dominio principale.	Indirizzo e-mail verificato in modo esplicito.	• I sottodomini ereditano la verifica dal dominio principale. • Indirizzo e-mail verificato in modo esplicito.
Livello di invio	Indirizzi e-mail limitati al semplice invio di e-mail.	L'indirizzo e-mail può essere utilizzato nell'invio avanzato*.	L'indirizzo e-mail può essere utilizzato nell'invio avanzato*.

	Solo dominio verificato	Solo indirizzo e-mail verificato	Sia il dominio che l'indirizzo e-mail verificati
Stato visualizzato	Stato console/API: • Domini/sottodomini = verificati • Indirizzo e-mail = non verificato.	Stato console/API: • Indirizzo e-mail = verificato	Stato console/API: • Domini/sottodomini = verificati • Indirizzo e-mail = verificato.

*L'invio avanzato include l'utilizzo dell'indirizzo e-mail con set di configurazione, autorizzazioni di policy per l'invio delegato e configurazioni che sovrascrivono le impostazioni del dominio.

Per inviare e-mail dallo stesso dominio o indirizzo e-mail in più di una regione Regione AWS, devi creare e verificare un'identità separata per ogni regione. Puoi verificare fino a un massimo di 10.000 identità in ciascuna Regione.

Quando si crea e si verificano le identità di un dominio e di un indirizzo e-mail, è necessario considerare gli aspetti seguenti:

- Puoi inviare e-mail da qualsiasi sottodominio o indirizzo e-mail del dominio verificato senza verificare singolarmente ciascuno di essi. Ad esempio, se crei e verifichi un'identità per example.com non avrai bisogno di creare identità separate per a.example.com, a.b.example.com, user@example.com, user@a.example.com e così via.
- Come specificato nello standard RFC 1034, ogni etichetta DNS può contenere fino a 63 caratteri e l'intero nome di dominio non può superare una lunghezza totale di 255 caratteri.
- Se verifichi un dominio, un sottodominio o un indirizzo e-mail che condivide un dominio root, le impostazioni delle identità verificate (come le notifiche di feedback) si applicano al livello più granulare verificato.
  - Le impostazioni dell'identità degli indirizzi e-mail verificati sostituiscono le impostazioni del dominio verificato.
  - Le impostazioni dell'identità dei sottodomini verificati sostituiscono le impostazioni di identità del dominio verificato e le impostazioni dei sottodomini di livello inferiore sostituiscono le impostazioni dei sottodomini di livello superiore.

Supponi ad esempio di verificare user@a.b.example.com, a.b.example.com, b.example.com ed example.com. Queste sono le impostazioni delle identità verificate che verranno utilizzate nei seguenti scenari:

- Le e-mail inviate da user@example.com (un indirizzo che non è specificamente verificato) utilizzeranno le impostazioni di example.com.
- Le e-mail inviate da user@a.b.example.com (un indirizzo che è specificamente verificato) utilizzeranno le impostazioni di user@a.b.example.com.
- Le e-mail inviate da user@b.example.com (un indirizzo che non è specificamente verificato) utilizzeranno le impostazioni di b.example.com.

- Puoi aggiungere etichette a indirizzi e-mail verificati senza eseguire ulteriori fasi di verifica. Per aggiungere un'etichetta a un indirizzo e-mail, aggiungi un segno più (+) tra il nome dell'account e il simbolo "at" (@), seguito da un'etichetta di testo. Ad esempio, se hai già verificato sender@example.com, puoi usare sender+myLabel@example.com come indirizzo "From" o "Return-Path" per le tue e-mail. Puoi usare questa funzione per implementare Variable Envelope Return Path (VERP). Quindi puoi usare VERP per rilevare e rimuovere dalle liste di distribuzione gli indirizzi e-mail non consegnabili.
- I nomi di dominio non distinguono tra maiuscole e minuscole. Se verifichi example.com, puoi inviare e-mail anche da EXAMPLE.com.
- Per gli indirizzi e-mail viene rilevata la distinzione tra maiuscole e minuscole. Se verifichi sender@EXAMPLE.com, non potrai inviare e-mail da sender@example.com, a meno che tu non verifichi anche sender@example.com.
- In ciascuna Regione AWS puoi verificare fino a un massimo di 10.000 identità (domini e indirizzi e-mail, in qualsiasi combinazione).

> **Tip**
>
> Se utilizzi SES per la prima volta, puoi utilizzare la procedura guidata introduttiva per creare e verificare la tua prima identità (indirizzo e-mail o dominio).

Indice

- Verifica di un'identità indirizzo e-mail
- Creare e verificare un'identità e contemporaneamente assegnare un set di configurazione di default
- Uso di modelli di e-mail di verifica personalizzati

Creazione di un'identità dominio

Parte della creazione di un'identità di dominio consiste nella configurazione della verifica basata su DKIM. DomainKeys Identified Mail (DKIM) è un metodo di autenticazione e-mail utilizzato da Amazon SES per verificare la proprietà del dominio e che i server di posta di ricezione utilizzano per convalidare l'autenticità delle e-mail. È possibile scegliere di configurare DKIM utilizzando Easy DKIM o Bring Your Own DKIM (BYODKIM) e, a seconda della scelta, sarà necessario configurare la lunghezza della chiave privata nel modo seguente:

- Easy DKIM: accetta il valore di default di Amazon SES di 2048 bit o sovrascrivilo selezionando 1024 bit.
- BYODKIM: la lunghezza della chiave privata deve essere almeno 1024 bit e fino a 2048 bit.

Consulta the section called “Lunghezza della chiave di firma DKIM” per ulteriori informazioni sulla lunghezza delle chiavi di firma DKIM e su come modificarle.

La procedura seguente illustra come creare un'identità di un dominio tramite la console Amazon SES.

- Se hai già creato il dominio e devi solo verificarlo, passa alla procedura the section called “Verifica di un'identità dominio” in questa pagina.

Creazione di un'identità del dominio

1. Accedi alla AWS Management Console e apri la console Amazon SES all'indirizzo https://console.aws.amazon.com/ses/.
2. Nel pannello di navigazione, in Configuration (Configurazione), scegli Verified identities (Identità verificate).
3. Scegli Create identity (Crea identità).
4. In Identity details (Dettagli identità), seleziona Domain (Dominio) come tipo di identità da creare. Per completare la procedura di verifica del dominio, devi accedere alle impostazioni DNS del dominio.
5. Immetti il nome del dominio o sottodominio nel campo Domain (Dominio).

> **Tip**
>
> Se il tuo dominio è www.example.com, inserisci example.com come dominio. Non includere "www." perché altrimenti il processo di verifica del dominio non avrà esito positivo.

6. (Opzionale) Per attivare l'opzione Assign a default configuration set (Assegna un set di configurazione predefinito), seleziona la relativa casella di controllo.

   1. Per Default configuration set (Set di configurazione predefinito), seleziona il set di configurazione esistente che desideri assegnare all'identità. Se non hai ancora creato set di configurazione, consulta Set di configurazione.

      > **Note**
      >
      > Amazon SES utilizza per impostazione predefinita il set di configurazione assegnato solo quando non viene specificato nessun altro set al momento dell'invio. Se viene specificato un set di configurazione, Amazon SES applica il set specificato al posto del set predefinito.

7. (Opzionale) Per attivare l'opzione Use a custom MAIL FROM domain (Usa dominio MAIL FROM personalizzato), seleziona la relativa casella di controllo e completa la procedura seguente. Per ulteriori informazioni, consulta the section called “Uso di un dominio MAIL FROM personalizzato”.

   1. Per MAIL FROM domain (Dominio MAIL FROM), immetti il dominio secondario che desideri utilizzare come dominio MAIL FROM. Questo deve corrispondere a un sottodominio dell'identità di dominio che stai verificando. Il dominio MAIL FROM non deve essere un dominio da cui invii e-mail.
   2. Per Behavior on MX failure (Comportamento in caso di errore MX), indica quale azione deve intraprendere Amazon SES se non riesce a trovare il record MX richiesto al momento dell'invio. Seleziona una delle seguenti opzioni:
      - Use default MAIL FROM domain (Usa il dominio MAIL FROM predefinito): se il record MX del dominio MAIL FROM personalizzato non è configurato correttamente, Amazon SES usa un sottodominio amazonses.com. Il sottodominio varia in base all'Regione AWS in cui è in uso Amazon SES.

- Rifiuta messaggio: se il registro MX del dominio MAIL FROM personalizzato non è configurato correttamente, Amazon SES restituisce un errore `MailFromDomainNotVerified`. Se scegli questa opzione, i messaggi e-mail che tenti di inviare da questo dominio vengono automaticamente rifiutati.

3. Per Publish DNS records to Route53 (Pubblica registri DNS su Route53), se il tuo dominio è ospitato tramite Amazon Route 53, hai la possibilità di consentire a SES di pubblicare i registri TXT e MX associati al momento della creazione lasciando Enabled (Abilitato) selezionato. Se preferisci pubblicare questi registri in un secondo momento, deseleziona la casella di controllo Enabled (Abilitato). Puoi tornare in un secondo momento per pubblicare i registri su Route 53 modificando l'identità, consulta the section called “Modifica di un'identità tramite la console”.

8. (Facoltativo) Per configurare una verifica personalizzata basata su DKIM al di fuori dell'impostazione predefinita SES che utilizza Easy DKIM con una lunghezza della firma a 2048 bit, in Verifying your domain (Verifica del dominio) espandi Advanced DKIM settings (Impostazioni avanzate di DKIM) e scegli il tipo di DKIM da configurare:

   a. Easy DKIM:

      i. Nel campo Identity type (Tipo di identità), scegli Easy DKIM.

      ii. Nel campo DKIM signing key length (Lunghezza chiave di firma DKIM), scegli RSA_2048_BIT o RSA_1024_BIT.

      iii. Per Publish DNS records to Route53 (Pubblica registri DNS su Route53), se il tuo dominio è ospitato tramite Amazon Route 53, hai la possibilità di consentire a SES di pubblicare i registri CNAME associati al momento della creazione lasciando Enabled (Abilitato) selezionato. Se preferisci pubblicare questi registri in un secondo momento, deseleziona la casella di controllo Enabled (Abilitato). Puoi tornare in un secondo momento per pubblicare i registri su Route 53 modificando l'identità, consulta the section called “Modifica di un'identità tramite la console”.

   b. Provide DKIM authentication token (BYODKIM) (Fornisci token di autenticazione DKIM (BYODKIM)):

      i. Assicurati di aver già generato una coppia di chiavi pubblica-privata e di aver aggiunto la chiave pubblica al tuo provider host DNS. Per ulteriori informazioni, consulta the section called “BYODKIM (Bring Your Own DKIM)”.

      ii. Nel campo Identity type (Tipo di identità), scegli Provide DKIM authentication token (BYODKIM) (Fornisci token di autenticazione DKIM) (BYODKIM)).

iii. Per Private key (Chiave privata), incolla la chiave privata generata dalla coppia di chiavi pubblica-privata. La chiave privata deve utilizzare almeno la crittografia RSA a 1024 bit e fino a 2048 bit e dev'essere codificata usando la codifica base64 (PEM).

> **Note**
>
> È necessario eliminare la prima e l'ultima riga (`-----BEGIN PRIVATE KEY-----` e `-----END PRIVATE KEY-----`, rispettivamente) della chiave privata generata. Inoltre, devi rimuovere le interruzioni di riga nella chiave privata generata. Il valore risultante è una stringa di caratteri senza spazi o interruzioni di riga.

iv. Per Selector name (Nome del selettore), inserisci il nome del selettore specificato nelle impostazioni DNS del tuo dominio.

9. Assicurati che la casella Enabled (Abilitate) sia selezionata nel campo DKIM signatures (Firme DKIM).
10. (Opzionale) Puoi aggiungere uno o più tag all'identità del dominio includendo una chiave di tag e un valore facoltativo per la chiave:
    1. Scegli Add new tag (Aggiungi nuovo tag) e immetti il valore per Key (Chiave). In alternativa, puoi aggiungere un valore al tag in Value (Valore).
    2. Ripeti l'operazione senza superare i 50 tag, oppure scegli Remove (Rimuovi) per rimuovere i tag.
11. Scegli Create identity (Crea identità).

Ora che hai creato e configurato la tua identità di dominio con DKIM, devi completare il processo di verifica con il tuo provider DNS: vai su the section called “Verifica di un'identità dominio” e segui le procedure di autenticazione DNS per il tipo di DKIM con cui hai configurato la tua identità.

Verifica dell'identità di un dominio DKIM con il provider DNS

Dopo aver creato l'identità del dominio configurata con DKIM, devi completare il processo di verifica con il provider DNS seguendo le procedure di autenticazione specifiche per il tipo di DKIM scelto.

Se non è stata creata un'identità di dominio, consulta the section called “Creazione di un'identità dominio”.

> **Note**
>
> La verifica di un'identità di dominio richiede l'accesso alle impostazioni DNS del dominio. La propagazione delle modifiche a queste impostazioni può richiedere fino a 72 ore.

Verifica dell'identità di un dominio DKIM con il provider DNS

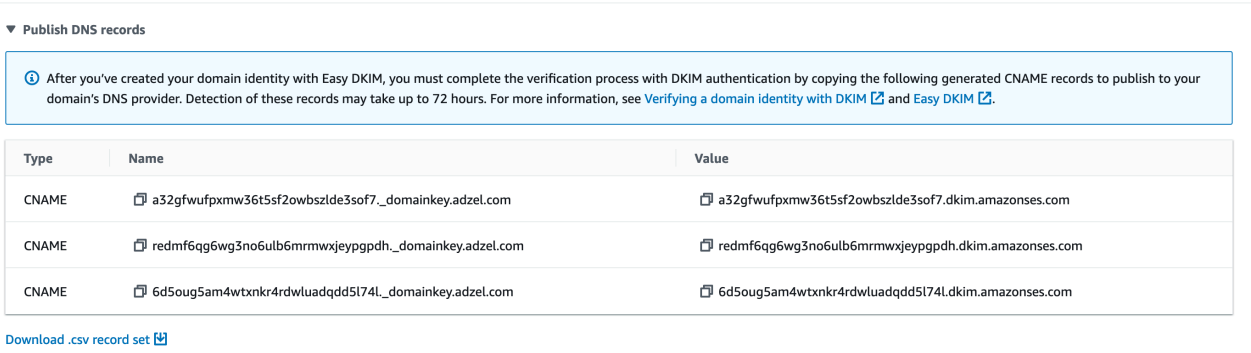
1. Nella tabella Loaded identities (Identità caricate), seleziona il dominio che desideri verificare.
2. Nella scheda Authentication (Autenticazione) della pagina di dettaglio delle identità, espandi Publish DNS records (Pubblica record DNS).
3. A seconda della versione di DKIM con cui hai configurato il tuo dominio, Easy DKIM o BYODKIM, segui le rispettive istruzioni:

   Easy DKIM

   Verifica di un dominio configurato con Easy DKIM

   1. Nella tabella Publish DNS records (Pubblica i record DNS), copia i tre registri CNAME che appaiono in questa sezione per la pubblicazione (l'aggiunta) nel tuo provider DNS. In alternativa, puoi scegliere Download .csv record set (Scarica il set di record .csv) per salvare una copia dei record sul tuo computer.

      L'immagine seguente mostra un esempio di registri CNAME da pubblicare nel provider DNS.

   2. Aggiungi i registri CNAME alle impostazioni DNS del tuo dominio in base al provider host DNS:

      - All DNS host providers (excluding Route 53) (Tutti i provider host DNS, escluso Route 53): effettua l'accesso al DNS o provider di hosting Web del dominio e aggiungi

i registri CNAME che contengono i valori copiati o salvati in precedenza. Diversi provider dispongono di procedure diverse per l'aggiornamento dei record DNS. Consulta la Tabella dei provider DNS/hosting per conoscere le procedure.

> **Note**
>
> Alcuni provider di DNS non consentono di includere trattini di sottolineatura (_) nei nomi di record. Tuttavia, la sottolineatura nel nome di record DKIM è obbligatoria. Se il provider di DNS non consente di inserire un segno di sottolineatura nel nome del record, contatta il team di assistenza clienti del provider per ricevere assistenza.

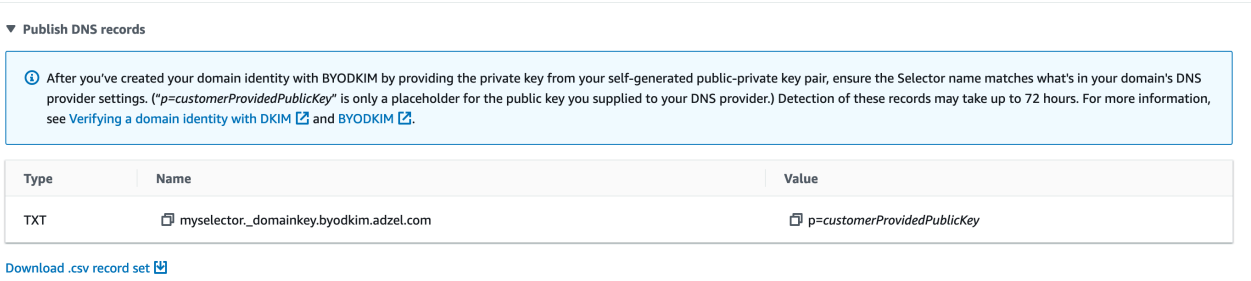
- Route 53 as your DNS host provider (Se utilizzi Route 53 come provider host DNS): se utilizzi Route 53 sullo stesso account che utilizzi per l'invio di e-mail mediante SES e il dominio è registrato, SES aggiorna automaticamente le impostazioni DNS per il tuo dominio se hai abilitato la pubblicazione al momento della creazione. Altrimenti, puoi pubblicare facilmente in Route 53 con un solo clic anche dopo la creazione: consulta the section called “Modifica di un'identità tramite la console”. Se le tue impostazioni DNS non si aggiornano automaticamente o desideri aggiungere record CNAME a Route 53 che non si trovano nello stesso account che usi per inviare e-mail tramite SES, completa le procedure in Modifica dei record.
- If you're not sure who your DNS provider is (Se non conosci il tuo provider DNS): rivolgiti al tuo amministratore di sistema per ulteriori informazioni.

BYODKIM

Per verificare un dominio configurato con BYODKIM

1. Per riassumere, quando hai creato il tuo dominio o hai configurato il dominio esistente con BYODKIM, hai aggiunto la chiave privata (dalla tua coppia di chiavi pubblica-privata autogenerata) e il prefisso del nome del selettore nei rispettivi campi nella pagina Impostazioni avanzate DKIM della console SES. Ora è necessario completare il processo di verifica aggiornando i seguenti registri per il provider host DNS.
2. Nella tabella Publish DNS records (Pubblica record DNS), copia il registro del nome del selettore visualizzato nella colonna Name (Nome) per la pubblicazione (l'aggiunta) nel tuo provider DNS. In alternativa, puoi scegliere Download .csv record set (Scarica il set di registri .csv) per salvare una copia dei registri sul tuo computer.

L'immagine seguente mostra un esempio di registro del nome del selettore da pubblicare nel provider DNS.



3. Accedi al DNS o provider di hosting Web del dominio e aggiungi il registro del nome del selettore copiato o salvato in precedenza. Diversi provider dispongono di procedure diverse per l'aggiornamento dei record DNS. Consulta la Tabella dei provider DNS/hosting per conoscere le procedure.

> **Note**
>
> Alcuni provider di DNS non consentono di includere trattini di sottolineatura (_) nei nomi di record. Tuttavia, la sottolineatura nel nome di record DKIM è obbligatoria. Se il provider di DNS non consente di inserire un segno di sottolineatura nel nome del record, contatta il team di assistenza clienti del provider per ricevere assistenza.

4. Se non lo hai già fatto, assicurati di aggiungere la chiave pubblica dalla tua coppia di chiavi pubblica-privata autogenerata al DNS o al provider di hosting Web del dominio.

   Nota: nella tabella Publish DNS records (Pubblica record DNS), il record della chiave pubblica che appare nella colonna Value (Valore) mostra solo "p=customerProvidedPublicKey" come segnaposto per la chiave pubblica che hai fornito al provider DNS.

> **Note**
>
> Quando pubblichi (aggiungi) la chiave pubblica al tuo provider DNS, questa deve essere formattata come segue:
>
> - È necessario eliminare la prima e l'ultima riga (`-----BEGIN PUBLIC KEY-----` e `-----END PUBLIC KEY-----`, rispettivamente) della chiave

pubblica generata. Inoltre, devi rimuovere le interruzioni di riga nella chiave pubblica generata. Il valore risultante è una stringa di caratteri senza spazi o interruzioni di riga.

- Devi includere il prefisso p= come mostrato nella colonna Value (Valore) nella tabella Publish DNS records (Pubblica record DNS).

4. La propagazione delle modifiche alle impostazioni DNS può richiedere fino a 72 ore. La procedura di verifica è completata quando Amazon SES rileva tutti i registri DKIM richiesti nelle impostazioni DNS del dominio. La DKIM configuration (Configurazione DKIM) del dominio viene visualizzata come Successful (Riuscita) e Identity status (Stato dell'identità) viene visualizzato come Verified (Verificato).
5. Per configurare e verificare un dominio MAIL FROM personalizzato, segui la procedura indicata in Configurazione del dominio MAIL FROM personalizzato.

Questa sezione include i collegamenti alla documentazione dei provider DNS più comunemente utilizzati. Questo elenco non è esaustivo e non significa approvazione; allo stesso modo, se il tuo provider DNS non è elencato, ciò non implica che tu non possa utilizzare il dominio con Amazon SES.

Provider DNS/di hosting	Collegamento alla documentazione
GoDaddy	Add a CNAME record (collegamento esterno)
DreamHost	How do I add custom DNS records? (collegamento esterno)
Cloudflare	Gestione dei record DNS in Cloudflare (collegamento esterno)
HostGator	Manage DNS Records with HostGator/eNom (collegamento esterno)
Namecheap	How do I add TXT/SPF/DKIM/DMARC records for my domain? (collegamento esterno)
Names.co.uk	Changing your domains DNS Settings (collegamento esterno)

Provider DNS/di hosting	Collegamento alla documentazione
Wix	Aggiungere o aggiornare i record CNAME nel tuo account Wix (collegamento esterno)

Risoluzione dei problemi di verifica del dominio

Se hai completato le procedure precedenti, ma dopo 72 ore il tuo dominio non è verificato, esegui le seguenti operazioni:

- Verifica di avere inserito i valori dei record DNS nei campi corretti. Alcuni provider DNS chiamano il campo Name/host (Nome/host) come Host o Hostname. Inoltre, alcuni provider chiamano il campo Record value (Valore del record) come Points to (Punta a) o Result (Risultato).
- Assicurati che il provider non abbia automaticamente aggiunto il nome del dominio al valore Name/host (Nome/host) immesso nel record DNS. Alcuni provider aggiungono il nome del dominio senza renderlo noto. Se il provider ha aggiunto il nome del dominio al valore Name/host (Nome/host), rimuovilo dalla fine del valore. Puoi anche provare ad aggiungere un punto alla fine del valore nel record DNS. Questo punto indica al provider che il nome di dominio è completo.
- Il carattere di sottolineatura (_) è obbligatorio nel valore Name/host (Nome/host) di ogni record DNS. Se il provider DNS non consente caratteri di sottolineatura nei nomi dei record DNS, contatta il supporto clienti del provider per ricevere assistenza.
- I record di convalida da aggiungere alla configurazione DNS dei domini variano per ogni Regione AWS. Se desideri utilizzare un dominio per inviare e-mail da più Regioni AWS, devi verificare l'identità del dominio separata per ogni Regione.

Creazione di un'identità dell'indirizzo e-mail

Per creare l'identità di un indirizzo e-mail utilizzando la console Amazon SES, completa la procedura che segue.

Per creare un'identità dell'indirizzo e-mail (console)

1. Accedi alla AWS Management Console e apri la console Amazon SES all'indirizzo https://console.aws.amazon.com/ses/.
2. Nel pannello di navigazione, in Configuration (Configurazione), scegli Verified identities (Identità verificate).

3. Scegli Create identity (Crea identità).
4. In Identity details (Dettagli identità), scegli Email address (Indirizzo e-mail) come tipo di identità che intendi creare.
5. Per Email address (Indirizzo e-mail), immetti l'indirizzo e-mail da usare. Deve essere un indirizzo a cui è possibile accedere e che può ricevere e-mail.
6. (Opzionale) Per attivare l'opzione Assign a default configuration set (Assegna un set di configurazione predefinito), seleziona la relativa casella di controllo.

    1. Per Default configuration set (Set di configurazione predefinito), seleziona il set di configurazione esistente che desideri assegnare all'identità. Se non hai ancora creato set di configurazione, consulta Set di configurazione.

    > **Note**
    >
    > Amazon SES utilizza per impostazione predefinita il set di configurazione assegnato solo quando non viene specificato nessun altro set al momento dell'invio. Se viene specificato un set di configurazione, Amazon SES applica il set specificato al posto del set predefinito.

7. (Opzionale) Puoi aggiungere uno o più tag all'identità del dominio includendo una chiave di tag e un valore facoltativo per la chiave:

    1. Scegli Add new tag (Aggiungi nuovo tag) e immetti il valore per Key (Chiave). In alternativa, puoi aggiungere un valore al tag in Value (Valore).
    2. Ripeti l'operazione senza superare i 50 tag, oppure scegli Remove (Rimuovi) per rimuovere i tag.
8. Per creare l'identità dell'indirizzo e-mail, scegli Create identity (Crea identità). Dopo la creazione, dovresti ricevere un'e-mail di verifica entro cinque minuti. Il passaggio successivo consiste nel verificare il tuo indirizzo e-mail seguendo la procedura di verifica nella sezione successiva.

> **Note**
>
> Puoi personalizzare i messaggi inviati agli indirizzi e-mail che hai provato a verificare. Per ulteriori informazioni, consulta the section called “Uso di modelli di e-mail di verifica personalizzati”.

Ora che hai creato l'identità dell'indirizzo e-mail, devi completare il processo di verifica - procedi con the section called “Verifica di un'identità indirizzo e-mail”.

Verifica di un'identità indirizzo e-mail

Dopo aver creato l'identità dell'indirizzo e-mail, è necessario completare il processo di verifica.

Se non è stata creata un'identità di un indirizzo e-mail, consulta the section called “Creazione di un'identità dell'indirizzo e-mail”.

Verifica di un'identità indirizzo e-mail

1. Controlla la casella di posta dell'indirizzo specificato per creare l'identità e individua l'e-mail ricevuta da no-reply-aws@amazon.com.
2. Apri l'e-mail e fai clic sul collegamento per completare la procedura di verifica relativa all'indirizzo e-mail. Al termine, Identity status (Stato dell'identità) diventa Verified (Verificato).

Risoluzione dei problemi di verifica di un indirizzo e-mail

Se non ricevi l'e-mail di verifica entro cinque minuti dalla creazione della tua identità, prova questa procedura di risoluzione dei problemi:

- Controlla di aver scritto l'indirizzo e-mail correttamente.
- Assicurati che l'indirizzo che stai tentando di verificare sia in grado di ricevere e-mail. A questo scopo, utilizza un altro indirizzo e-mail per inviare un'e-mail di testo all'indirizzo che desideri verificare.
- Controlla la cartella di posta indesiderata.
- Il link nell'e-mail di verifica scade dopo 24 ore. Per inviare una nuova e-mail di verifica, scegli Resend (Rinvio) nella parte superiore della pagina dei dettagli dell'identità.

Creare e verificare un'identità e contemporaneamente assegnare un set di configurazione di default

Puoi utilizzare l'operazione CreateEmailIdentity nell'API Amazon SES v2 per creare una nuova identità e-mail e impostare contemporaneamente il relativo set di configurazione di default.

> **Note**
>
> Prima di completare le procedure in questa sezione, è necessario prima installare e configurare l'AWS CLI. Per ulteriori informazioni, consulta la AWS Command Line InterfaceGuida per l'utente di .

Per impostare un set di configurazione di default tramite la AWS CLI

- Nella riga di comando, inserisci il comando seguente per utilizzare l'operazione CreateEmailIdentity.

```
aws sesv2 create-email-identity --email-identity ADDRESS-OR-DOMAIN --configuration-set-name CONFIG-SET
```

Nei comandi precedenti, sostituisci *ADDRESS-OR-DOMAIN* con l'identità e-mail che desideri verificare. Sostituisci *CONFIG-SET* con il nome del set di configurazione che desideri impostare come set di configurazione di default dell'identità.

Se l'esecuzione del comando riesce, l'operazione viene completata senza fornire output.

Per verificare il tuo indirizzo e-mail

1. Controlla la casella di posta in arrivo dell'indirizzo e-mail che stai verificando. Riceverai un messaggio con l'oggetto seguente: "Amazon Web Services - Richiesta di verifica indirizzo e-mail nella regione *RegionName*," dove *RegionName* è il nome della regione Regione AWS nella quale hai tentato di verificare l'indirizzo e-mail.

   Apri il messaggio e quindi fai clic sul collegamento in esso contenuto.

   > **Note**
   >
   > Il collegamento contenuto nel messaggio di verifica scade 24 ore dopo l'invio del messaggio. Trascorse 24 ore dalla ricezione dell'e-mail di verifica, ripeti le fasi 1-5 per ricevere un messaggio di verifica con un collegamento valido.

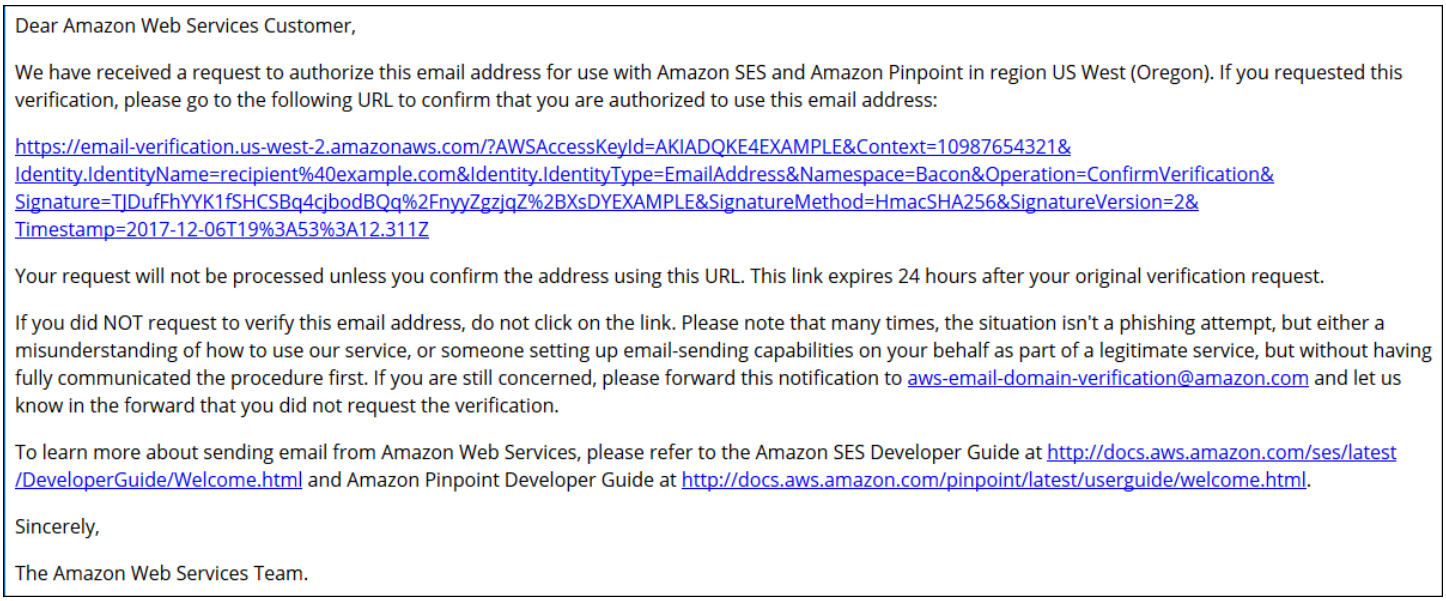
2. Nella console Amazon SES in Gestione identità scegli Indirizzi e-mail. Individua nell'elenco l'indirizzo e-mail che stai verificando. Se l'indirizzo e-mail è stato verificato, il valore nella colonna Status (Stato) è "verified" (verificato).

Per verificare il tuo dominio

Se hai inserito un nome di dominio per il parametro `--email-identity` nella procedura della riga di comando precedente, consulta Verifica di un'identità dominio per ulteriori informazioni.

Uso di modelli di e-mail di verifica personalizzati

Quando si tenta di verificare un indirizzo e-mail, Amazon SES invia all'indirizzo un'e-mail simile all'esempio illustrato nell'immagine che segue.



Dear Amazon Web Services Customer,

We have received a request to authorize this email address for use with Amazon SES and Amazon Pinpoint in region US West (Oregon). If you requested this verification, please go to the following URL to confirm that you are authorized to use this email address:

https://email-verification.us-west-2.amazonaws.com/?AWSAccessKeyId=AKIADQKE4EXAMPLE&Context=10987654321&Identity.IdentityName=recipient%40example.com&Identity.IdentityType=EmailAddress&Namespace=Bacon&Operation=ConfirmVerification&Signature=TJDufFhYYK1fSHCSBq4cjbodBQq%2FnyyZgzjqZ%2BXsDYEXAMPLE&SignatureMethod=HmacSHA256&SignatureVersion=2&Timestamp=2017-12-06T19%3A53%3A12.311Z

Your request will not be processed unless you confirm the address using this URL. This link expires 24 hours after your original verification request.

If you did NOT request to verify this email address, do not click on the link. Please note that many times, the situation isn't a phishing attempt, but either a misunderstanding of how to use our service, or someone setting up email-sending capabilities on your behalf as part of a legitimate service, but without having fully communicated the procedure first. If you are still concerned, please forward this notification to aws-email-domain-verification@amazon.com and let us know in the forward that you did not request the verification.

To learn more about sending email from Amazon Web Services, please refer to the Amazon SES Developer Guide at http://docs.aws.amazon.com/ses/latest/DeveloperGuide/Welcome.html and Amazon Pinpoint Developer Guide at http://docs.aws.amazon.com/pinpoint/latest/userguide/welcome.html.

Sincerely,

The Amazon Web Services Team.

Diversi clienti Amazon SES creano applicazioni (ad esempio sistemi di ticketing o suite di e-mail marketing) che inviano e-mail tramite Amazon SES per conto dei propri clienti. Per gli utenti finali di queste applicazioni, la procedura di verifica dell'e-mail può essere poco chiara: l'e-mail di verifica usa il marchio Amazon SES, anziché il marchio dell'applicazione e gli utenti finali non hanno mai effettuato la registrazione per utilizzare direttamente Amazon SES.

Se il tuo caso d'uso di Amazon SES richiede la verifica degli indirizzi e-mail dei clienti per l'uso con Amazon SES, puoi creare messaggi e-mail di verifica personalizzati. Queste e-mail personalizzate rendono la procedura più chiara per i clienti, consentendo loro di completare la registrazione più rapidamente.

> **Note**
>
> Per utilizzare questa funzione, il tuo account Amazon SES deve essere fuori dalla sandbox. Per ulteriori informazioni, consulta Richiedi l'accesso alla produzione (uscita dalla sandbox di Amazon SES).

Argomenti in questa sezione:

- Creazione di un modello di e-mail di verifica personalizzato
- Modifica di un modello di e-mail di verifica personalizzato
- Invio di e-mail di verifica mediante modelli personalizzati
- Domande frequenti relative all'e-mail di verifica personalizzata

Creazione di un modello di e-mail di verifica personalizzato

Per creare un messaggio e-mail di verifica personalizzato, usa l'operazione API `CreateCustomVerificationEmailTemplate`. Questa operazione accetta i seguenti input:

Attributo	Descrizione
`TemplateName`	Il nome del modello. Il nome specificato deve essere univoco.
`FromEmailAddress`	L'indirizzo e-mail da cui viene inviata l'e-mail di verifica. Per poter essere utilizzato con il tuo account Amazon SES, l'indirizzo o il dominio specificato deve essere verificato. **Note** L'attributo `FromEmailAddress` non supporta i nomi di visualizzazione (noti anche come nomi "friendly from").
`TemplateSubject`	La riga dell'oggetto dell'e-mail di verifica.
`TemplateContent`	Il corpo dell'e-mail. Il corpo dell'e-mail può contenere HTML, con alcune restrizioni. Per ulteriori informazioni, consulta Domande frequenti relative all'e-mail di verifica personalizzata.

Attributo	Descrizione
`SuccessRedirectionURL`	L'URL a cui gli utenti vengono inviati se la verifica dei loro indirizzi e-mail riesce.
`FailureRedirectionURL`	L'URL a cui gli utenti vengono inviati se la verifica dei loro indirizzi e-mail non riesce.

Puoi usare gli SDK AWS o l'AWS CLI per creare un modello di e-mail di verifica personalizzato con l'operazione `CreateCustomVerificationEmailTemplate`. Per ulteriori informazioni sugl SDK AWS, consulta la pagina relativa agli strumenti per Amazon Web Service. Per ulteriori informazioni sull'AWS CLI, consulta Interfaccia a riga di comando di AWS.

La sezione seguente include le procedure per creare un messaggio e-mail di verifica personalizzato utilizzando AWS CLI. Le procedure si basano sul presupposto che siano già state eseguite l'installazione e la configurazione dell'AWS CLI. Per ulteriori informazioni sull'installazione e la configurazione dell'AWS CLI, consulta la Guida per l'utente di AWS Command Line Interface.

> **Note**
>
> Per completare la procedura descritta in questa sezione, è necessario utilizzare la versione 1.14.6 o successiva dell'AWS CLI. Per ottenere risultati ottimali, eseguire l'aggiornamento alla versione più recente dell'AWS CLI. Per informazioni sull'installazione o sull'aggiornamento dell'AWS CLI, consulta la pagina relativa a Installazione di AWS Command Line Interface nella Guida per l'utente di AWS Command Line Interface.

1. In un editor di testo, crea un nuovo file. Incolla il contenuto seguente nell'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**
>
> Per semplificare la lettura dell'esempio precedente, l'attributo `TemplateContent` contiene interruzioni di riga. Se incolli l'esempio precedente in un file di testo, rimuovi le interruzioni di riga prima di continuare.

Sostituisci i valori di `TemplateName`, `FromEmailAddress`, `TemplateSubject`, `TemplateContent`, `SuccessRedirectionURL` e `FailureRedirectionURL` con i valori personalizzati.

> **Note**
>
> L'indirizzo e-mail specificato per il parametro `FromEmailAddress` deve essere verificato o deve essere un indirizzo su un dominio verificato. Per ulteriori informazioni, consulta Identità verificate in Amazon SES.

Al termine, salva il file come `customverificationemail.json`.

2. Alla riga di comando, digita il comando seguente per creare il modello di e-mail di verifica personalizzato:

```
aws sesv2 create-custom-verification-email-template --cli-input-json file://
customverificationemail.json
```

3. (Opzionale) Puoi confermare che il modello è stato creato digitando il comando seguente:

```
aws sesv2 list-custom-verification-email-templates
```

Modifica di un modello di e-mail di verifica personalizzato

È possibile modificare un modello di e-mail di verifica personalizzato utilizzando l'operazione `UpdateCustomVerificationEmailTemplate`. Questa operazione accetta gli stessi input dell'operazione `CreateCustomVerificationEmailTemplate` (ovvero gli attributi `TemplateName`, `FromEmailAddress`, `TemplateSubject`, `TemplateContent`, `SuccessRedirectionURL` e `FailureRedirectionURL`). Tuttavia, con l'operazione `UpdateCustomVerificationEmailTemplate`, nessuno di questi attributi è necessario. Quando per `TemplateName` passi un valore uguale a quello di un modello di e-mail di verifica personalizzato esistente, gli attributi specificati sovrascrivono quelli originariamente presenti nel modello.

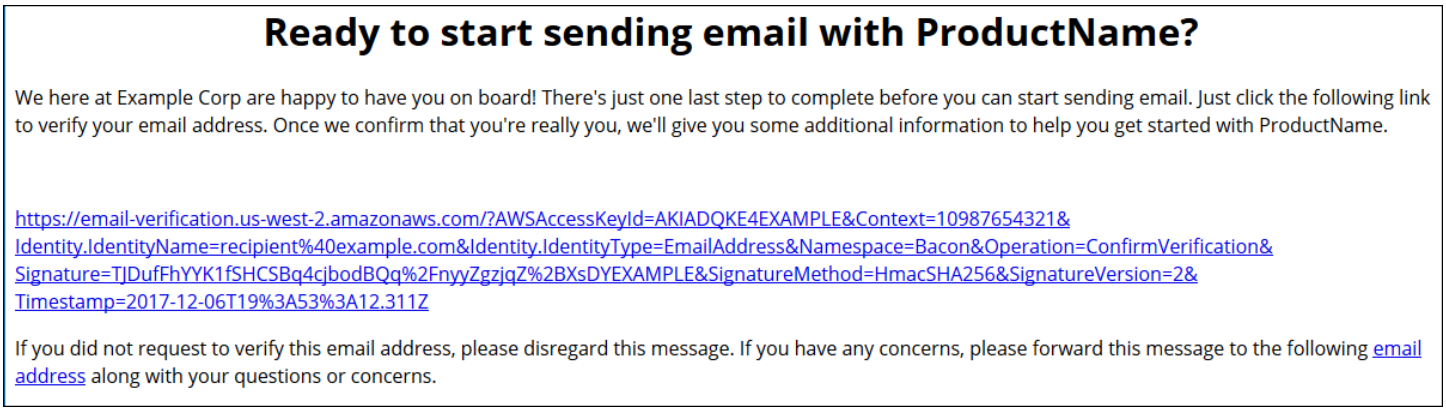
Invio di e-mail di verifica mediante modelli personalizzati

Dopo aver creato almeno un modello di e-mail di verifica personalizzato, puoi inviarlo ai tuoi clienti chiamando l'operazione API SendCustomVerificationEmail. Puoi chiamare l'operazione `SendCustomVerificationEmail` utilizzando gli SDK AWS o l'AWS CLI. L'operazione `SendCustomVerificationEmail` accetta i seguenti input:

Attributo	Descrizione
`EmailAddress`	L'indirizzo e-mail sottoposto a verifica.
`TemplateName`	Nome del modello di e-mail di verifica personalizzato inviato all'indirizzo e-mail sottoposto a verifica.
`ConfigurationSetName`	(Opzionale) Il nome di un set di configurazione da utilizzare per l'invio dell'e-mail di verifica.

Supponi, ad esempio, che i tuoi clienti effettuino la registrazione al servizio utilizzando un modulo disponibile nell'applicazione. Quando il cliente completa il modulo e lo invia, l'applicazione chiama l'operazione `SendCustomVerificationEmail`, passando l'indirizzo e-mail del cliente e il nome del modello che desideri utilizzare.

Il cliente riceve un'e-mail che usa il modello di e-mail personalizzato da te creato. Amazon SES aggiunge automaticamente un collegamento al destinatario e una breve dichiarazione di non responsabilità. L'immagine seguente mostra un esempio di verifica e-mail che usa il modello creato in Creazione di un modello di e-mail di verifica personalizzato.



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.

Domande frequenti relative all'e-mail di verifica personalizzata

Questa sezione contiene le risposte alle domande frequenti sulla funzionalità del modello di e-mail di verifica personalizzato.

D1. Quanti modelli di e-mail di verifica personalizzati è possibile creare?

Per ogni account Amazon SES è possibile creare fino a 50 modelli di e-mail di verifica personalizzati.

D2. Come si presenta ai destinatari l'e-mail di verifica personalizzata?

Le e-mail di verifica personalizzate includono il contenuto specificato durante la creazione del modello, seguito da un collegamento su cui i destinatari devono fare clic per verificare il propri indirizzo e-mail.

D3. Posso visualizzare l'anteprima del messaggio e-mail di verifica personalizzato?

Per visualizzare l'anteprima di un messaggio e-mail di verifica personalizzato, usa l'operazione `SendCustomVerificationEmail` per inviare un messaggio e-mail di verifica a un indirizzo di tua proprietà. Se non fai clic sul collegamento di verifica, Amazon SES non crea una nuova identità. Se invece fai clic sul collegamento di verifica, puoi eliminare l'identità appena creata utilizzando l'operazione `DeleteIdentity`.

D4. Posso includere immagini nel modelli di e-mail di verifica personalizzati?

È possibile incorporare immagini nell'HTML per i tuoi modelli utilizzando la codifica base64. Quando si incorporano le immagini in questo modo, Amazon SES le converte automaticamente in allegati. Puoi codificare un'immagine nella riga di comando mediante uno dei seguenti comandi:

Linux, macOS, or Unix

```
base64 -i imagefile.png | tr -d '\n' > output.txt
```

Windows

```
certutil -encodehex -f imagefile.png output.txt 0x40000001
```

Sostituisci *imagefile.png* con il nome del file che desideri codificare. In entrambi i comandi in alto l'immagine con codifica base64 viene salvata in `output.txt`.

È possibile incorporare l'immagine con codifica base64 includendo quanto segue nel file HTML per il modello: `<img src="`*base64EncodedImage*`"/>`

Nell'esempio, sostituisci *png* con il tipo di file dell'immagine codificata (ad esempio jpg o gif) e *base64EncodedImage* con l'immagine con codifica base64 (ovvero il contenuto di `output.txt` da uno dei comandi precedenti).

D5. Sono previste limitazioni per il contenuto incluso nei modelli di e-mail di verifica personalizzati?

Le dimensioni dei modelli di e-mail di verifica personalizzati non possono superare 10 MB. Inoltre, i modelli di e-mail di verifica personalizzati che contengono HTML possono utilizzare solo i tag gli attributi elencati nella tabella seguente.

Tag HTML	Attributi consentiti
`abbr`	`class, id, style, title`
`acronym`	`class, id, style, title`
`address`	`class, id, style, title`
`area`	`class, id, style, title`

Tag HTML	Attributi consentiti
b	class, id, style, title
bdo	class, id, style, title
big	class, id, style, title
blockquote	cite, class, id, style, title
body	class, id, style, title
br	class, id, style, title
button	class, id, style, title
caption	class, id, style, title
center	class, id, style, title
cite	class, id, style, title
code	class, id, style, title
col	class, id, span, style, title, width
colgroup	class, id, span, style, title, width
dd	class, id, style, title
del	class, id, style, title
dfn	class, id, style, title
dir	class, id, style, title
div	class, id, style, title
dl	class, id, style, title

Tag HTML	Attributi consentiti
dt	class, id, style, title
em	class, id, style, title
fieldset	class, id, style, title
font	class, id, style, title
form	class, id, style, title
h1	class, id, style, title
h2	class, id, style, title
h3	class, id, style, title
h4	class, id, style, title
h5	class, id, style, title
h6	class, id, style, title
head	class, id, style, title
hr	class, id, style, title
html	class, id, style, title
i	class, id, style, title
img	align, alt, class, height, id, src, style, title, width
input	class, id, style, title
ins	class, id, style, title
kbd	class, id, style, title
label	class, id, style, title

Tag HTML	Attributi consentiti
legend	class, id, style, title
li	class, id, style, title
map	class, id, style, title
menu	class, id, style, title
ol	class, id, start, style, title, type
optgroup	class, id, style, title
option	class, id, style, title
p	class, id, style, title
pre	class, id, style, title
q	cite, class, id, style, title
s	class, id, style, title
samp	class, id, style, title
select	class, id, style, title
small	class, id, style, title
span	class, id, style, title
strike	class, id, style, title
strong	class, id, style, title
sub	class, id, style, title
sup	class, id, style, title

Tag HTML	Attributi consentiti
table	class, id, style, summary, title, width
tbody	class, id, style, title
td	abbr, axis, class, colspan, id, rowspan, style, title, width
textarea	class, id, style, title
tfoot	class, id, style, title
th	abbr, axis, class, colspan, id, rowspan, scope, style, title, width
thead	class, id, style, title
tr	class, id, style, title
tt	class, id, style, title
u	class, id, style, title
ul	class, id, style, title, type
var	class, id, style, title

> **Note**
>
> I modelli di e-mail di verifica personalizzati non possono includere tag di commento.

D6. Quanti indirizzi e-mail verificati possono esistere nel mio account?

Ogni account Amazon SES supporta fino a 10.000 identità verificate in ciascuna Regione AWS. In Amazon SES le identità includono sia domini sia indirizzi e-mail verificati.

D7. Posso creare modelli di e-mail di verifica personalizzati utilizzando la console Amazon SES?

Al momento è possibile creare, modificare ed eliminare e-mail di verifica personalizzate solo utilizzando l'API Amazon SES.

D8. Posso tenere traccia degli eventi di apertura e clic che si verificano quando i clienti ricevono e-mail di verifica personalizzate?

Le e-mail di verifica personalizzate non possono includere la traccia di apertura e clic.

D9. Le e-mail di verifica personalizzate possono includere intestazioni personalizzate?

Le e-mail di verifica personalizzate non possono includere intestazioni personalizzate.

D10. Posso rimuovere il testo visualizzato nella parte inferiore delle e-mail di verifica personalizzate?

Al termine di ogni e-mail di verifica personalizzata viene aggiunto automaticamente il testo seguente, che non può essere rimosso:

Se non hai richiesto di verificare questo indirizzo e-mail, ignora questo messaggio.

D11. Le e-mail di verifica personalizzate sono con firma DKIM?

Perché le e-mail di verifica siano provviste di firma DKIM, è necessario che l'indirizzo e-mail specificato nell'attributo `FromEmailAddress` quando si crea il modello di e-mail di verifica sia configurato per generare una firma DKIM. Per ulteriori informazioni sulla configurazione di DKIM per domini e indirizzi e-mail, consulta the section called “Autenticazione delle e-mail con DKIM”.

D12. Perché le operazioni API relative al modello di e-mail di verifica personalizzato non appaiono nell'SDK o nella CLI?

Se non sei in grado di utilizzare le operazioni relative al modello di e-mail di verifica personalizzato in un SDK o nell'AWS CLI, potresti utilizzare una versione obsoleta dell'SDK o della CLI. Le operazioni relative al modello di e-mail di verifica personalizzato sono disponibili nei seguenti SDK e CLI:

- Versione 1.14.6 o successive di AWS Command Line Interface
- Versione 3.3.205.0 o successive di AWS SDK for .NET
- Versione 1.3.20170531.19 o successive dell'SDK AWS per C++.
- Versione 1.12.43 o successive di AWS SDK for Go
- Versione 1.11.245 o successive di AWS SDK for Java
- Versione 2.166.0 o successive di AWS SDK for JavaScript

- Versione 3.45.2 o successive di AWS SDK for PHP
- Versione 1.5.1 o successive di AWS SDK for Python (Boto)
- Versione 1.5.0 o successiva della gemma `aws-sdk-ses` in AWS SDK for Ruby

D13. Perché ricevo errori **`ProductionAccessNotGranted`** quando invio e-mail di verifica personalizzate?

L'errore `ProductionAccessNotGranted` indica che l'account si trova ancora nella sandbox Amazon SES. Puoi inviare e-mail di verifica personalizzate solo se l'account è stato rimosso dalla sandbox. Per ulteriori informazioni, consulta Richiedi l'accesso alla produzione (uscita dalla sandbox di Amazon SES).

Gestione delle identità in Amazon SES

Nella console Amazon SES, puoi visualizzare un elenco di identità, aprire un'identità per visualizzarne e modificarne le impostazioni dei dettagli, associare un set di configurazione di default o eliminare una o più identità.

> **Note**
>
> Le procedure descritte in questa sezione si applicano solo alle identità nell'Regione AWS selezionata. Per gestire le identità create in più di una Regione, ripeti le procedure per ogni Regione AWS.

Visualizzazione di un elenco delle identità in Amazon SES

È possibile usare l'API o la console Amazon SES per visualizzare un elenco di identità di dominio e indirizzo e-mail verificati o in attesa di verifica. Puoi anche visualizzare gli identificativi per i quali la verifica non ha avuto esito positivo.

Per visualizzare le identità del dominio e dell'indirizzo e-mail (console)

1. Accedi alla AWS Management Console e apri la console Amazon SES all'indirizzo https://console.aws.amazon.com/ses/.
2. Nella console, utilizza il selettore della Regione per scegliere l'Regione AWS per cui desideri visualizzare l'elenco di identità.

> **Note**
>
> Questa procedura consente di visualizzare solo un elenco di identità per l'Regione AWS selezionata.

3. Nel pannello di navigazione, in Configuration (Configurazione), scegli Verified identities (Identità verificate). La tabella Loaded identities (Identità caricate) mostra le identità di dominio e di indirizzo e-mail. La colonna Status (Stato) indica se un'identità è stata verificata, è in attesa di verifica o non ha superato il processo di verifica. Le definizioni di tutti i possibili valori dello stato sono riportate di seguito:

   - Verified (Verificata): l'identità è stata verificata correttamente per l'invio in SES.
   - Failure (Errore): SES non è stato in grado di verificare l'identità. Se si tratta di un dominio, significa che SES non è stato in grado di rilevare i registri DNS entro 72 ore. Se si tratta di un indirizzo e-mail, significa che l'e-mail di verifica inviata all'indirizzo e-mail non è stata confermata entro 24 ore.
   - Pending (In attesa): SES sta ancora cercando di verificare l'identità.
   - Temporary Failure (Errore temporaneo): per un dominio verificato in precedenza, SES verificherà periodicamente il registro DNS richiesto per la verifica. Se a un certo punto SES non è in grado di rilevare il registro, lo stato cambierà in Temporary Failure (Errore temporaneo). SES effettuerà una nuova verifica del registro DNS per 72 ore e, in caso di mancato rilevamento del registro, lo stato del dominio cambierà in Failure (Errore). Se invece riuscirà a rilevare il registro, lo stato del dominio cambierà in Verified (Verificato).
   - Not started (Non avviato): non hai ancora avviato il processo di verifica.
4. Per ordinare le identità in base allo stato di verifica, seleziona la colonna Status (Stato).
5. Per visualizzare la pagina dei dettagli di un'identità, seleziona l'identità che intendi visualizzare.

Eliminazione di un'identità in Amazon SES

Puoi utilizzare la console o l'API di Amazon SES per rimuovere l'identità di un dominio o di un indirizzo e-mail dal tuo account nell'Regione AWS selezionata.

Per rimuovere l'identità di un dominio o di un indirizzo e-mail (console)

1. Accedi alla AWS Management Console e apri la console Amazon SES all'indirizzo https://console.aws.amazon.com/ses/.

2. Nella console, utilizza il selettore della Regione per scegliere l'Regione AWS da cui desideri eliminare una o più identità.
3. Nel pannello di navigazione, in Configuration (Configurazione), scegli Verified identities (Identità verificate).

   La tabella Loaded identities (Identità caricate) mostra un elenco di identità di dominio e indirizzo e-mail.
4. Nella colonna Identity (Identità), seleziona l'identità che desideri eliminare. È possibile eliminare più identità selezionando la casella accanto a ogni identità da eliminare.
5. Seleziona Delete (Elimina).

Modifica di un'identità esistente in Amazon SES

Puoi utilizzare la console o l'API di Amazon SES per modificare l'identità di un dominio o di un indirizzo e-mail nel tuo account nella Regione AWS selezionata.

Per modificare l'identità di un dominio o di un indirizzo e-mail (console)

1. Accedi alla AWS Management Console e apri la console Amazon SES all'indirizzo https://console.aws.amazon.com/ses/.
2. Nella console, utilizza il selettore della Regione per scegliere la Regione AWS da cui desideri modificare una o più identità.
3. Nel pannello di navigazione, in Configuration (Configurazione), scegli Verified identities (Identità verificate).

   La tabella Loaded identities (Identità caricate) mostra un elenco di identità di dominio e indirizzo e-mail.
4. Nella colonna Identity (Identità), seleziona l'identità che desideri modificare (facendo clic direttamente sul nome dell'identità anziché selezionandone la casella di controllo).
5. Nella pagina dei dettagli dell'identità, seleziona la scheda contenente le categorie che desideri modificare.
6. In uno dei container categorici della scheda selezionata, scegli il pulsante Edit (Modifica) dell'attributo che desideri modificare, apporta le modifiche, quindi scegli Save changes (Salva modifiche).

a. Se desideri modificare gli attributi nella scheda Authentication (Autenticazione) e la tua identità di dominio è ospitata in Amazon Route 53 e non hai ancora pubblicato i suoi registri DNS, sarà presente un pulsante Publish DNS records to Route53 (Pubblica registri DNS su Route53) accanto al pulsante Edit (Modifica) in uno o entrambi i container DomainKeys Identified Mail (DKIM) o Custom MAIL FROM domain (Dominio MAIL FROM personalizzato).

> **Note**
>
> La scheda Authentication (Autenticazione) è presente solo quando il tuo account dispone di un dominio verificato o di un indirizzo e-mail che utilizza un dominio verificato nel tuo account.

b. Puoi pubblicare i registri DNS direttamente dal pulsante Publish DNS records to Route53 (Pubblica registri DNS su Route53): è sufficiente fare clic su di esso, verrà visualizzato un banner di conferma e il pulsante Publish DNS records to Route53 (Pubblica registri DNS su Route53) non sarà più visibile per il relativo container.

7. Ripeti i passaggi 5 e 6 per ogni attributo dell'identità che desideri modificare.

Modifica un'identità per utilizzare un set di configurazione predefinito utilizzando l'API

Puoi utilizzare l'operazione PutEmailIdentityConfigurationSetAttributes per aggiungere o rimuovere un set di configurazione predefinito da un'identità e-mail esistente.

> **Note**
>
> Prima di completare le procedure in questa sezione, è necessario prima installare e configurare l'AWS CLI. Per ulteriori informazioni, consulta la Guida per l'utente AWS Command Line Interface.

Per aggiungere un set di configurazione di default tramite la AWS CLI

- Nella riga di comando, inserisci il comando seguente per utilizzare l'operazione PutEmailIdentityConfigurationSetAttributes.

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

Nei comandi precedenti, sostituisci *ADDRESS-OR-DOMAIN* con l'identità e-mail che desideri verificare. Sostituisci *CONFIG-SET* con il nome del set di configurazione che desideri impostare come set di configurazione di default dell'identità.

Se l'esecuzione del comando riesce, l'operazione viene completata senza fornire output.

Per rimuovere un set di configurazione di default tramite la AWS CLI

- Nella riga di comando, inserisci il comando seguente per utilizzare l'operazione PutEmailIdentityConfigurationSetAttributes.

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

Nei comandi precedenti, sostituisci *ADDRESS-OR-DOMAIN* con l'identità e-mail che desideri verificare.

Se l'esecuzione del comando riesce, l'operazione viene completata senza fornire output.

Recupera il set di configurazione di default utilizzato dall'identità (API)

Puoi utilizzare l'operazione GetEmailIdentity per restituire il set di configurazione di default per un'identità e-mail, se applicabile.

> **Note**
>
> Prima di completare le procedure in questa sezione, è necessario prima installare e configurare l'AWS CLI. Per ulteriori informazioni, consulta la Guida per l'utente AWS Command Line Interface.

Per restituire un set di configurazione di default tramite la AWS CLI

- Nella riga di comando, inserisci il comando seguente per utilizzare l'operazione GetEmailIdentity.

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

Nei comandi precedenti, sostituisci *ADDRESS-OR-DOMAIN* con l'identità e-mail per la quale desideri conoscere il set di configurazione di default, se presente.

Se il comando viene eseguito correttamente, fornisce a un oggetto JSON i dettagli dell'identità e-mail.

Sovrascrivi il set di configurazione di default corrente utilizzato dall'identità (API)

Puoi utilizzare l'operazione SendEmail per inviare e-mail con un set di configurazione diverso. In tal caso, il set di configurazione che specifichi sovrascrive il set di configurazione di default per l'identità.

> **Note**
>
> Prima di completare le procedure in questa sezione, è necessario prima installare e configurare l'AWS CLI. Per ulteriori informazioni, consulta la Guida per l'utente AWS Command Line Interface.

Per sovrascrivere un set di configurazione di default tramite la AWS CLI

- Nella riga di comando, inserisci il comando seguente per utilizzare l'operazione SendEmail.

```
aws sesv2 send-email --destination file://DESTINATION-JSON --content file://CONTENT-JSON --from-email-address ADDRESS-OR-DOMAIN --configuration-set-name CONFIG-SET
```

Nei comandi precedenti, sostituisci *DESTINATION-JSON* con il file JSON di destinazione, *CONTENT-JSON* con il file JSON del contenuto, *ADDRESS-OR-DOMAIN* con il tuo indirizzo e-mail FROM e *CONFIG-SET* con il nome del set di configurazione che desideri utilizzare al posto del set di configurazione di default per l'identità.

Se il comando viene eseguito correttamente, emette un `MessageId`.

Configurazione delle identità in Amazon SES

Amazon Simple Email Service (Amazon SES) utilizza il protocollo SMTP (Simple Mail Transfer Protocol) per l'invio di e-mail. Poiché il protocollo SMTP non prevede autenticazione, gli spammer possono inviare messaggi e-mail apparentemente provenienti da qualcun altro, nascondendo l'origine

reale. Attraverso la falsificazione delle intestazioni delle e-mail e lo spoofing degli indirizzi IP di origine, gli spammer possono indurre i destinatari a credere che i messaggi ricevuti siano autentici.

La maggior parte degli ISP che inoltrano il traffico e-mail prendono misure per valutare se i messaggi siano legittimi. Una delle misure prese dagli ISP è determinare se un'e-mail sia autenticata. L'autenticazione richiede che i mittenti verifichino di essere proprietari dell'account da cui effettuano l'invio. In alcuni casi, gli ISP rifiutano di inoltrare e-mail che non sono autenticate. Per assicurare un'efficienza del recapito ottimale, è consigliabile autenticare le e-mail.

Le sezioni seguenti descrivono due meccanismi di autenticazione utilizzati dagli ISP, Sender Policy Framework (SPF) e DomainKeys Identified Mail (DKIM), oltre a fornire istruzioni su come utilizzare questi standard con Amazon SES.

- Per informazioni su SPF, che fornisce un modo per tracciare un messaggio e-mail fino al sistema da cui è stato inviato, consulta Autenticazione delle e-mail con SPF in Amazon SES.
- Per informazioni su DKIM, uno standard che consente di firmare i messaggi e-mail per mostrare agli ISP che sono legittimi e non sono stati modificati in transito, consulta Autenticazione delle e-mail con DKIM in Amazon SES.
- Per informazioni su come assicurare la conformità al sistema Domain-based Message Authentication, Reporting and Conformance (DMARC), che si basa su SPF e DKIM, consulta Conformità al protocollo di autenticazione DMARC in Amazon SES.

Metodi di autenticazione delle e-mail

Amazon Simple Email Service (Amazon SES) utilizza il protocollo SMTP (Simple Mail Transfer Protocol) per l'invio di e-mail. Poiché il protocollo SMTP non prevede autenticazione, gli spammer possono inviare messaggi e-mail apparentemente provenienti da qualcun altro, nascondendo l'origine reale. Attraverso la falsificazione delle intestazioni delle e-mail e lo spoofing degli indirizzi IP di origine, gli spammer possono indurre i destinatari a credere che i messaggi ricevuti siano autentici.

La maggior parte degli ISP che inoltrano il traffico e-mail prendono misure per valutare se i messaggi siano legittimi. Una delle misure prese dagli ISP è determinare se un'e-mail sia autenticata. L'autenticazione richiede che i mittenti verifichino di essere proprietari dell'account da cui effettuano l'invio. In alcuni casi, gli ISP rifiutano di inoltrare e-mail che non sono autenticate. Per assicurare un'efficienza del recapito ottimale, è consigliabile autenticare le e-mail.

Indice

- Autenticazione delle e-mail con SPF in Amazon SES
- Uso di un dominio MAIL FROM personalizzato
- Conformità al protocollo di autenticazione DMARC in Amazon SES
- Utilizzo di BIMI in Amazon SES

Autenticazione delle e-mail con DKIM in Amazon SES

DomainKeys Identified Mail (DKIM) è uno standard di sicurezza delle e-mail progettato per assicurarsi che un'e-mail che afferma di provenire da un dominio specifico sia stata effettivamente autorizzata dal proprietario di quel dominio. Utilizza la crittografia a chiave pubblica per firmare un'e-mail con una chiave privata. I server destinatari possono quindi utilizzare una chiave pubblica pubblicata nel DNS di un dominio per verificare che le parti del messaggio di posta elettronica non siano state modificate durante il transito.

Le firme DKIM sono opzionali. Puoi decidere di firmare le tue e-mail utilizzando una firma DKIM per migliorare la capacità di recapitare i messaggi con gli ISP conformi allo standard DKIM. Amazon SES offre due opzioni per firmare i messaggi utilizzando una firma DKIM:

- Easy DKIM: SES genera una coppia di chiavi pubblica-privata e aggiunge automaticamente una firma DKIM per ogni messaggio inviato da tale identità, consulta Easy DKIM in Amazon SES.
- BYODKIM (Bring Your Own DKIM): fornisci la tua coppia di chiavi pubblica-privata e SES aggiunge una firma DKIM per ogni messaggio inviato da tale identità, consulta Specifica del proprio token di autenticazione DKIM (BYODKIM) in Amazon SES.
- Aggiunta manuale della firma DKIM: aggiungi la tua firma DKIM a ogni e-mail che invii utilizzando l'API `SendRawEmail`, consulta Firma DKIM manuale in Amazon SES.

Lunghezza della chiave di firma DKIM

Poiché molti provider DNS ora supportano completamente la crittografia DKIM a 2048 bit RSA, Amazon SES supporta anche DKIM 2048 per consentire un'autenticazione più sicura delle e-mail e, quindi, la utilizza come lunghezza predefinita della chiave quando configuri Easy DKIM dall'API o dalla console. Le chiavi a 2048 bit possono essere configurate e utilizzate in BYODKIM (Bring Your Own DKIM), in cui la lunghezza della chiave di firma deve essere di almeno 1024 bit e di massimo 2048 bit.

Per motivi di sicurezza e di recapitabilità della posta elettronica, in caso di configurazione con Easy DKIM, puoi scegliere di utilizzare le lunghezze di chiave a 1024 e 2048 bit insieme alla flessibilità di

tornare a 1024 nel caso in cui ci siano problemi causati da provider DNS che ancora non supportano 2048. Nella creazione di una nuova identità, questa verrà creata con DKIM 2048 per impostazione predefinita, a meno che non specifichi 1024.

Per preservare la capacità di recapitare i messaggi di posta elettronica in transito, esistono restrizioni sulla frequenza con cui è possibile modificare la lunghezza della chiave DKIM. Le restrizioni includono le seguenti:

- Non è possibile passare alla stessa lunghezza della chiave già configurata.
- Non è possibile passare a una lunghezza di chiave diversa più di una volta in un periodo di 24 ore (a meno che non si tratti del primo downgrade a 1024 in quel periodo).

Quando la tua e-mail è in transito, DNS utilizza la tua chiave pubblica per autenticare la tua e-mail; pertanto, se cambi le chiavi troppo rapidamente o frequentemente, il DNS potrebbe non essere in grado di effettuare l'autenticazione DKIM della tua e-mail in quanto la chiave precedente potrebbe già essere invalidata, quindi queste restrizioni impediscono che ciò accada.

Considerazioni su DKIM

Quando utilizzi DKIM per autenticare il tuo indirizzo e-mail, vengono applicate le regole seguenti:

- Devi configurare DKIM solo per il dominio che usi nel tuo indirizzo "Da". Non devi configurare DKIM per i domini che utilizzi negli indirizzi "Percorso di ritorno" o "Rispondi a".
- Amazon SES è disponibile in diverse regioni AWS. Se utilizzi più di una regione AWS per l'invio di e-mail, devi completare il processo di configurazione di DKIM in ciascuna regione per assicurarti che tutte le tue e-mail siano provviste di firma DKIM.
- Poiché le proprietà DKIM vengono ereditate dal dominio padre, quando effettui la verifica di un dominio con autenticazione DKIM:
  - L'autenticazione DKIM si applica anche a tutti i sottodomini di quel dominio.
    - Le impostazioni DKIM per un sottodominio consentono di sovrascrivere le impostazioni per il dominio padre, permettendo di disabilitare l'ereditarietà (se non desideri che il sottodominio utilizzi l'autenticazione DKIM) e di riabilitarla in un secondo momento.
  - L'autenticazione DKIM si applica anche a tutte le e-mail inviate da un'identità e-mail che fa riferimento al dominio verificato DKIM nel rispettivo indirizzo.
    - Le impostazioni DKIM per un indirizzo e-mail consentono di sovrascrivere le impostazioni per il sottodominio (se applicabile) e il dominio padre, permettendo di disabilitare l'ereditarietà (se desideri inviare e-mail senza l'autenticazione DKIM) e di riabilitarla in un secondo momento.

Informazioni sulle proprietà della firma DKIM ereditate

È importante comprendere innanzitutto che un'identità di indirizzo e-mail eredita le proprietà della firma DKIM dal proprio dominio padre se quest'ultimo è stato configurato con DKIM, indipendentemente dal fatto che sia stato utilizzato Easy DKIM o BYODKIM. Pertanto, la disabilitazione o l'abilitazione della firma DKIM sull'identità dell'indirizzo e-mail, in effetti, sovrascrive le proprietà della firma DKIM del dominio in base a questi fattori chiave:

- Se hai già configurato DKIM per il dominio a cui appartiene l'indirizzo e-mail, non è necessario abilitare la firma DKIM anche per l'identità dell'indirizzo e-mail.
  - Quando configuri DKIM per un dominio, Amazon SES esegue automaticamente l'autenticazione di ogni e-mail da ogni indirizzo di tale dominio, attraverso le proprietà DKIM ereditate per il dominio padre.
- Le impostazioni DKIM per un'identità di indirizzo e-mail specifica sovrascrivono automaticamente le impostazioni del dominio padre o del sottodominio (se applicabile) cui l'indirizzo appartiene.

Poiché le proprietà della firma DKIM dell'identità dell'indirizzo e-mail vengono ereditate dal dominio padre, se prevedi di sovrascriverle, devi tenere presente le regole gerarchiche di sovrascrittura, come spiegato nella tabella seguente.

Firma DKIM disabilitata per il dominio padre	Il dominio padre ha la firma DKIM abilitata
Non è possibile abilitare la firma di DKIM sull'identità dell'indirizzo e-mail.	Puoi disabilitare la firma di DKIM sull'identità dell'indirizzo e-mail.
	Puoi abilitare nuovamente la firma DKIM sull'identità dell'indirizzo e-mail.

In genere non è consigliabile disabilitare la firma DKIM, in quanto rischia di compromettere la reputazione del mittente e aumenta il rischio che la posta inviata venga trasferita nelle cartelle della posta indesiderata o dello spam o che il dominio venga falsificato.

Tuttavia, esiste la possibilità di sovrascrivere le proprietà della firma DKIM ereditate dal dominio sull'identità di un indirizzo e-mail per eventuali casi d'uso particolari o decisioni aziendali esterne per cui sia necessario disabilitare in modo permanente o temporaneo la firma DKIM o abilitarla nuovamente in un secondo momento. Per informazioni, consultare the section called “Sovrascrittura della firma DKIM ereditata su un indirizzo e-mail”.

Easy DKIM in Amazon SES

Quando imposti Easy DKIM per un'identità di dominio, Amazon SES aggiunge automaticamente una chiave DKIM a 2048 bit per ogni e-mail che invii da quell'identità. Puoi configurare Easy DKIM usando la console Amazon SES oppure usando l'API.

> **Note**
>
> Per configurare Easy DKIM, devi modificare le impostazioni DNS per il tuo dominio. Se utilizzi Route 53 come provider di DNS, Amazon SES è in grado di creare automaticamente i registri appropriati per te. Se utilizzi un altro provider di DNS, consulta la documentazione del provider per ulteriori informazioni sulla modifica delle impostazioni DNS per il tuo dominio.

> **Warning**
>
> Se attualmente è abilitato BYODKIM e stai passando a Easy DKIM, tieni presente che Amazon SES non utilizzerà BYODKIM per firmare le tue e-mail mentre Easy DKIM è in fase di configurazione e il tuo stato DKIM è in sospeso. Tra il momento in cui effettui la chiamata per abilitare Easy DKIM (tramite l'API o la console) e il momento in cui SES può confermare la configurazione DNS, le e-mail potrebbero essere inviate da SES senza una firma DKIM. Pertanto, si consiglia di utilizzare un passaggio intermedio per migrare da un metodo di firma DKIM all'altro (ad esempio, utilizzando un sotto dominio del dominio con BYODKIM abilitato e quindi eliminarlo una volta superata la verifica Easy DKIM) o eseguire questa attività durante l'eventuale tempo di inattività dell'applicazione.

Configurazione di Easy DKIM per un'identità di dominio verificata

La procedura di questa sezione è semplificata per mostrare solo i passaggi necessari per configurare Easy DKIM su un'identità di dominio che hai già creato. Se non hai ancora creato un'identità del dominio o vuoi visualizzare tutte le opzioni disponibili per personalizzare l'identità di un dominio, ad esempio l'utilizzo di un set di configurazione predefinito, del dominio MAIL FROM personalizzato e dei tag, consulta the section called “Creazione di un'identità dominio”.

Parte della creazione di un'identità di dominio Easy DKIM consiste nella configurazione della verifica basata su DKIM, in cui avrai la possibilità di accettare il valore predefinito di Amazon SES di 2.048 bit o di modificarlo selezionando 1.024 bit. Consulta the section called “Lunghezza della chiave di firma DKIM” per ulteriori informazioni sulla lunghezza delle chiavi di firma DKIM e su come modificarle.

Configurazione di Easy DKIM per un dominio

1. Accedere alla AWS Management Console e aprire la console Amazon SES all'indirizzo https://console.aws.amazon.com/ses/.
2. Nel pannello di navigazione, in Configuration (Configurazione), scegli Verified identities (Identità verificate).
3. Nell'elenco di identità scegli un'identità in cui l'opzione Identity type (Tipo di identità) è Domain (Dominio).

   > **Note**
   >
   > Per creare o verificare un dominio, consulta Creazione di un'identità dominio.

4. Nella scheda Authentication (Autenticazione), nel container DomainKeys Identified Mail (DKIM), scegli Edit (Modifica).
5. Nel container Advanced DKIM settings (Impostazioni avanzate di DKIM), scegli il pulsante Easy DKIM nel campo Identity type (Tipo di identità).
6. Nel campo DKIM signing key length (Lunghezza chiave di firma DKIM), scegli RSA_2048_BIT o RSA_1024_BIT.
7. Nel campo DKIM signatures (Firme DKIM), seleziona la casella Enabled (Abilitate).
8. Scegliere Save changes (Salva modifiche).
9. Ora che hai configurato la tua identità di dominio con Easy DKIM, devi completare il processo di verifica con il tuo provider DNS: a tale scopo, vvai su the section called “Verifica di un'identità dominio” e segui le procedure di autenticazione DNS per Easy DKIM.

Modifica della lunghezza della chiave di firma DKIM Easy per un'identità

La procedura descritta in questa sezione mostra come modificare facilmente i bit DKIM Easy necessari per l'algoritmo di firma. Mentre una lunghezza di firma di 2048 bit è sempre preferibile per la protezione avanzata che offre, potrebbero verificarsi situazioni che richiedono l'utilizzo della lunghezza di 1024 bit, ad esempio la necessità di utilizzare un provider DNS che supporta solo DKIM 1024.

Per preservare la capacità di recapitare i messaggi di posta elettronica in transito, esistono restrizioni sulla frequenza con cui è possibile modificare o ripristinare la lunghezza della chiave DKIM.

Quando la tua e-mail è in transito, DNS utilizza la tua chiave pubblica per autenticare la tua e-mail; pertanto, se cambi le chiavi troppo rapidamente o frequentemente, il DNS potrebbe non essere in grado di effettuare l'autenticazione DKIM della tua e-mail in quanto la chiave precedente potrebbe già essere invalidata, quindi le seguenti restrizioni impediscono che ciò accada:

- Non puoi passare alla stessa lunghezza della chiave già configurata.
- Non è possibile passare a una lunghezza di chiave diversa più di una volta in un periodo di 24 ore (a meno che non si tratti del primo downgrade a 1024 in quel periodo).

Utilizzando le procedure seguenti per modificare la lunghezza della chiave, se violi una di queste restrizioni, la console restituirà un banner di errore che indica che l'input fornito non è valido, insieme al motivo per cui non è valido.

Modifica dei bit di lunghezza della chiave di firma DKIM

1. Accedere alla AWS Management Console e aprire la console Amazon SES all'indirizzo https://console.aws.amazon.com/ses/.
2. Nel pannello di navigazione, in Configuration (Configurazione), scegli Verified identities (Identità verificate).
3. Nell'elenco di identità, scegli l'identità per la quale desideri modificare la lunghezza della chiave di firma Easy DKIM.
4. Nella scheda Authentication (Autenticazione), nel container DomainKeys Identified Mail (DKIM), scegli Edit (Modifica).
5. Nel container Advanced DKIM settings (Impostazioni avanzate di DKIM), scegli RSA_2048_BIT o RSA_1024_BIT nel campo DKIM signing key length (Lunghezza della chiave di firma DKIM).
6. Scegliere Save changes (Salva modifiche).

Specifica del proprio token di autenticazione DKIM (BYODKIM) in Amazon SES

In alternativa all'utilizzo di Easy DKIM, è possibile configurare l'autenticazione DKIM utilizzando la propria coppia di chiavi pubblica-privata. Questo processo è noto come Bring Your Own DKIM (BYODKIM).

Con BYODKIM, è possibile utilizzare un singolo record DNS per configurare l'autenticazione DKIM per i domini, contrariamente a Easy DKIM, che richiede la pubblicazione di tre record DNS separati. Inoltre, l'utilizzo di BYODKIM consente di ruotare le chiavi DKIM per i domini tutte le volte che lo si desidera.

Argomenti in questa sezione:

> **Warning**
>
> Se attualmente hai abilitato Easy DKIM e stai passando a BYODKIM, tieni presente che Amazon SES non utilizzerà Easy DKIM per firmare le tue e-mail mentre BYODKIM è in fase di configurazione e il tuo stato DKIM è in sospeso. Tra il momento in cui effettui la chiamata per abilitare BYODKIM (tramite l'API o la console) e il momento in cui SES può confermare la configurazione DNS, le e-mail potrebbero essere inviate da SES senza una firma DKIM. Pertanto, si consiglia di utilizzare un passaggio intermedio per migrare da un metodo di firma DKIM all'altro (ad esempio, utilizzando un sotto dominio del dominio con Easy DKIM abilitato e quindi eliminarlo una volta superata la verifica BYODKIM) o eseguire questa attività durante l'eventuale tempo di inattività dell'applicazione.

Fase 1: creazione della coppia di chiavi

Per utilizzare la funzione Bring Your Own DKIM, devi prima creare una coppia di chiavi RSA.

La chiave privata generata deve essere nel formato PKCS #1 o PKCS #8, utilizzare almeno la crittografia RSA a 1024 bit e fino a 2048 bit ed essere codificata utilizzando la codifica base64 (PEM). Consulta the section called “Lunghezza della chiave di firma DKIM” per ulteriori informazioni sulla lunghezza delle chiavi di firma DKIM e su come modificarle.

> **Note**
>
> È possibile utilizzare applicazioni e strumenti di terze parti per generare coppie di chiavi RSA a condizione che la chiave privata venga generata con almeno la crittografia RSA a 1024 bit e fino a 2048 bit ed sia codificata usando la base64 (PEM).

Nella procedura seguente, il codice di esempio che utilizza il comando `openssl genrsa` integrato nella maggior parte dei sistemi operativi Linux, macOS o Unix per creare la coppia di chiavi utilizzerà automaticamente la codifica base64 (PEM).

Creazione della coppia di chiavi dalla riga di comando Linux, macOS o Unix

1. Nella riga di comando, immetti il comando seguente per generare la chiave privata sostituendo *nnnn* con una lunghezza di almeno 1024 bit e fino a 2048:

   ```
   openssl genrsa -f4 -out private.key nnnn
   ```

2. Nella riga di comando, immetti il comando seguente per generare la chiave pubblica:

   ```
   openssl rsa -in private.key -outform PEM -pubout -out public.key
   ```

Fase 2: aggiunta del selettore e della chiave pubblica alla configurazione del dominio del provider DNS

Una volta creata una coppia di chiavi, è necessario aggiungere la chiave pubblica alla configurazione DNS per il dominio come record TXT.

Aggiunta della chiave pubblica alla configurazione DNS per il dominio

1. Accedi alla console di gestione del provider DNS o di hosting.
2. Aggiunta di un record MX alla configurazione DNS per il dominio Il record deve utilizzare il seguente formato:

Nome	Type (Tipo)	Value (Valore)
selettore ._chiaved ominio.*esempio.com*	TXT	p=*tuaChiavePubblica*

   In questo esempio, apporta le modifiche seguenti:

   - Sostituisci *selettore* con un nome univoco che identifichi la chiave.

> **Note**
>
> Alcuni provider di DNS non consentono di includere trattini di sottolineatura (_) nei nomi di record. Tuttavia, la sottolineatura nel nome di record DKIM è obbligatoria. Se il provider di DNS non consente di inserire un segno di sottolineatura nel nome del record, contatta il team di assistenza clienti del provider per ricevere assistenza.

- Sostituisci *esempio.com* con il tuo dominio.
- Sostituisci *yourPublicKey* con la chiave pubblica creata in precedenza e includi il prefisso p= come mostrato nella colonna Value (Valore) in alto.

> **Note**
>
> Quando pubblichi (aggiungi) la chiave pubblica al tuo provider DNS, questa deve essere formattata come segue:
>
> - È necessario eliminare la prima e l'ultima riga (`-----BEGIN PUBLIC KEY-----` e `-----END PUBLIC KEY-----`, rispettivamente) della chiave pubblica generata. Inoltre, devi rimuovere le interruzioni di riga nella chiave pubblica generata. Il valore risultante è una stringa di caratteri senza spazi o interruzioni di riga.
> - È necessario includere il prefisso p= come mostrato nella colonna Value (Valore) nella tabella qui sopra.

Diversi provider dispongono di procedure diverse per l'aggiornamento dei record DNS. La tabella che segue include i collegamenti alla documentazione dei provider DNS più comunemente utilizzati. Questo elenco non è esaustivo e non significa approvazione; allo stesso modo, se il tuo provider DNS non è elencato, ciò non implica che tu non possa utilizzare il dominio con Amazon SES.

Provider DNS/di hosting	Collegamento alla documentazione
Amazon Route 53	Modifica dei record nella Guida per sviluppatori di Amazon Route 53.
GoDaddy	Add a TXT record (collegamento esterno)

Provider DNS/di hosting	Collegamento alla documentazione
DreamHost	How do I add custom DNS records? (collegamento esterno)
Cloudflare	Gestione dei record DNS in Cloudflare (collegamento esterno)
HostGator	Manage DNS Records with HostGator/eNom (collegamento esterno)
Namecheap	How do I add TXT/SPF/DKIM/DMARC records for my domain? (collegamento esterno)
Names.co.uk	Changing your domains DNS Settings (collegamento esterno)
Wix	Aggiunta o aggiornamento di record TXT nell'account Wix (collegamento esterno)

Fase 3: configurazione e verifica di un dominio per utilizzare BYODKIM

È possibile impostare BYODKIM sia per i nuovi domini (ovvero i domini che attualmente non vengono utilizzati per inviare messaggi di posta elettronica tramite Amazon SES) che per quelli esistenti (ovvero i domini già configurati per l'utilizzo con Amazon SES) tramite al console o l'AWS CLI. Prima di completare le procedure con l'AWS CLI in questa sezione, è necessario prima installare e configurare l'AWS CLI. Per ulteriori informazioni, consulta la Guida per l'utente di AWS Command Line Interface.

Opzione 1: creazione di una nuova identità di dominio che utilizza BYODKIM

Questa sezione contiene una procedura per la creazione di una nuova identità di dominio che utilizza BYODKIM. Una nuova identità di dominio è un dominio che non è stato configurato in precedenza per inviare messaggi di posta elettronica utilizzando Amazon SES.

Se desideri configurare un dominio esistente per utilizzare BYODKIM, completa invece la procedura in Opzione 2: configurazione di un'identità di dominio esistente.

Creazione di un'identità usando BYODKIM dalla console

- Segui le procedure indicate in Creazione di un'identità dominio e, quando arrivi al passaggio 8, segui le istruzioni specifiche per BYODKIM.

Creazione di un'identità usando BYODKIM dall'AWS CLI

Per impostare un nuovo dominio, utilizza l'operazione `CreateEmailIdentity` nell'API Amazon SES.

1. Nell'editor, incollare il seguente codice:

```
{
    "EmailIdentity":"example.com",
    "DkimSigningAttributes":{
        "DomainSigningPrivateKey":"privateKey",
        "DomainSigningSelector":"selector"
    }
}
```

   In questo esempio, apporta le modifiche seguenti:

   - Sostituisci *`example.com`* con il dominio che desideri creare.
   - Sostituisci *`privateKey`* con la tua chiave privata.

     > **Note**
     >
     > È necessario eliminare la prima e l'ultima riga (`-----BEGIN PRIVATE KEY-----` e `-----END PRIVATE KEY-----`, rispettivamente) della chiave privata generata. Inoltre, devi rimuovere le interruzioni di riga nella chiave privata generata. Il valore risultante è una stringa di caratteri senza spazi o interruzioni di riga.

   - Sostituisci *`selector`* con il selettore univoco specificato al momento della creazione del record TXT nella configurazione DNS per il dominio.

   Al termine, salva il file come `create-identity.json`.

2. Nella riga di comando, inserisci il comando seguente:

```
aws sesv2 create-email-identity --cli-input-json file://path/to/create-identity.json
```

Nel comando precedente, sostituisci *path/to/create-identity.json* con il percorso al file creato nella fase precedente.

Opzione 2: configurazione di un'identità di dominio esistente

Questa sezione contiene le procedure per l'aggiornamento di un'identità di dominio esistente per l'utilizzo di BYODKIM. Un'identità di dominio esistente è un dominio già configurato per l'invio di messaggi di posta elettronica utilizzando Amazon SES.

Aggiornamento di un'identità usando BYODKIM dalla console

1. Accedi alla AWS Management Console e apri la console Amazon SES all'indirizzo https://console.aws.amazon.com/ses/.
2. Nel pannello di navigazione, in Configuration (Configurazione), scegli Verified identities (Identità verificate).
3. Nell'elenco di identità scegli un'identità in cui l'opzione Identity type (Tipo di identità) è Domain (Dominio).

> **Note**
>
> Per creare o verificare un dominio, consulta Creazione di un'identità dominio.

4. Nella scheda Authentication (Autenticazione), nel riquadro DomainKeys Identified Mail (DKIM), scegli Edit (Modifica).
5. Nel riquadro Advanced DKIM settings (Impostazioni avanzate di DKIM), scegli il pulsante Provide DKIM authentication token (Fornisci token di autenticazione DKIM) nel campo Identity type (Tipo di identità).
6. Per Private key (Chiave privata) incolla la chiave privata generata in precedenza.

> **Note**
>
> È necessario eliminare la prima e l'ultima riga (`-----BEGIN PRIVATE KEY-----` e `-----END PRIVATE KEY-----`, rispettivamente) della chiave privata generata. Inoltre,

devi rimuovere le interruzioni di riga nella chiave privata generata. Il valore risultante è una stringa di caratteri senza spazi o interruzioni di riga.

7. Per Selector name (Nome del selettore), indica il nome del selettore specificato nelle impostazioni DNS del dominio.
8. Nel campo DKIM signatures (Firme DKIM), seleziona la casella Enabled (Abilitate).
9. Seleziona Salva modifiche.

Aggiornamento di un'identità usando BYODKIM dall'AWS CLI

Per configurare un dominio esistente, utilizza l'operazione `PutEmailIdentityDkimSigningAttributes` nell'API Amazon SES.

1. Nell'editor, incollare il seguente codice:

```
{
    "SigningAttributes":{
        "DomainSigningPrivateKey":"privateKey",
        "DomainSigningSelector":"selector"
    },
    "SigningAttributesOrigin":"EXTERNAL"
}
```

In questo esempio, apporta le modifiche seguenti:

- Sostituisci *`privateKey`* con la tua chiave privata.

> **Note**
>
> È necessario eliminare la prima e l'ultima riga (`-----BEGIN PRIVATE KEY-----` e `-----END PRIVATE KEY-----`, rispettivamente) della chiave privata generata. Inoltre, devi rimuovere le interruzioni di riga nella chiave privata generata. Il valore risultante è una stringa di caratteri senza spazi o interruzioni di riga.

- Sostituisci *`selector`* con il selettore univoco specificato al momento della creazione del record TXT nella configurazione DNS per il dominio.

Al termine, salva il file come `update-identity.json`.

2. Nella riga di comando, inserisci il comando seguente:

```
aws sesv2 put-email-identity-dkim-signing-attributes --email-identity example.com
 --cli-input-json file://path/to/update-identity.json
```

   Nel comando precedente, apporta le modifiche seguenti:

   - Sostituisci *path/to/update-identity.json* con il percorso completo del file creato nella fase precedente.
   - Sostituisci *example.com* con il dominio che desideri aggiornare.

Verifica dello stato DKIM per un dominio che utilizza BYODKIM

Per verificare lo stato DKIM di un dominio dalla console

Dopo aver configurato un dominio per utilizzare BYODKIM, è possibile utilizzare la console SES per confermare che DKIM sia configurato correttamente.

1. Accedi alla AWS Management Console e apri la console Amazon SES all'indirizzo https://console.aws.amazon.com/ses/.
2. Nel pannello di navigazione, in Configuration (Configurazione), scegli Verified identities (Identità verificate).
3. Nell'elenco di identità, scegli l'identità per la quale desideri verificare lo stato DKIM.
4. La propagazione delle modifiche alle impostazioni DNS può richiedere fino a 72 ore. La procedura di verifica è completata quando Amazon SES rileva tutti i registri DKIM richiesti nelle impostazioni DNS del dominio. Se tutto è stato configurato correttamente, il campo DKIM configuration (Configurazione DKIM) del tuo dominio visualizza Successful (Riuscito) nel riquadro DomainKeys Identified Mail (DKIM) e il campo Identity status (Stato dell'identità) visualizza Verified (Verificato) nel riquadro Summary (Riepilogo).

Per verificare lo stato DKIM di un dominio utilizzando AWS CLI

Dopo aver configurato un dominio per utilizzare BYODKIM, è possibile utilizzare l'operazione GetEmailIdentity per verificare che DKIM sia configurato correttamente.

- Nella riga di comando, inserisci il comando seguente:

```
aws sesv2 get-email-identity --email-identity example.com
```

Nel comando precedente, sostituisci *example.com* con il dominio.

Questo comando restituisce un oggetto JSON contenente una sezione analoga al seguente esempio.

```
{
    ...
    "DkimAttributes": {
        "SigningAttributesOrigin": "EXTERNAL",
        "SigningEnabled": true,
        "Status": "SUCCESS",
        "Tokens": [ ]
    },
    ...
}
```

Se tutte le condizioni seguenti sono vere, BYODKIM è configurato correttamente per il dominio:

- Il valore della proprietà `SigningAttributesOrigin` è `EXTERNAL`.
- Il valore di `SigningEnabled` è `true`.
- Il valore di `Status` è `SUCCESS`.

Gestione di Easy DKIM e BYODKIM

Sono disponibili due metodi per gestire le impostazioni di DKIM per le tue identità autenticate con Easy DKIM o BYODKIM: la console Amazon SES basata sul Web e l'API Amazon SES. Puoi usare uno di questi metodi per ottenere i registri DKIM per un'identità oppure per abilitare o disabilitare la firma DKIM per un'identità.

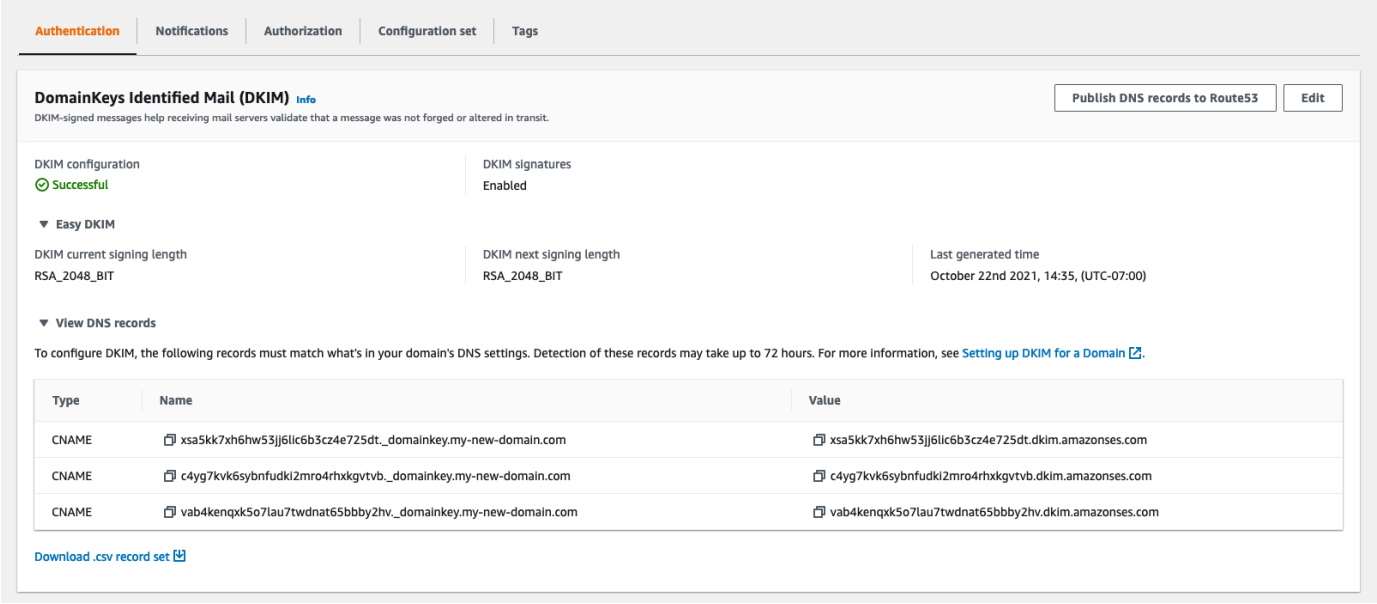
Ottenimento dei registri DKIM per un'identità

Puoi ottenere i registri DKIM per il tuo dominio o indirizzo e-mail in qualsiasi momento tramite la console Amazon SES.

Ottenimento dei registri DKIM per un'identità tramite la console

1. Accedi AWS Management Console e apri la console Amazon SES all'indirizzo https://console.aws.amazon.com/ses/.
2. Nel pannello di navigazione, in Configuration (Configurazione), scegli Verified identities (Identità verificate).
3. Nell'elenco delle identità, scegli quella per la quale desideri ottenere i registri DKIM.
4. Nella scheda Authentication (Autenticazione) della pagina di dettaglio delle identità, espandi View DNS records (Mostra record DNS).
5. Copia i tre registri CNAME (se hai utilizzato Easy DKIM) o il registro TXT (se hai usato BYODKIM) che appaiono in questa sezione. In alternativa, puoi scegliere Download .csv record set (Scarica il set di record .csv) per salvare una copia dei record sul tuo computer.

   L'immagine seguente mostra un esempio della sezione View DNS records (Mostra registri DNS) ampliata che rivela i registri CNAME associati a Easy DKIM.



Puoi inoltre ottenere i registri DKIM per un'identità tramite l'API Amazon SES. Un metodo comune di interazione con l'API è rappresentato dall'utilizzo dell' AWS CLI.

Per ottenere i record DKIM per un'identità utilizzando il AWS CLI

1. Nella riga di comando, digita il comando seguente:

```
aws ses get-identity-dkim-attributes --identities "example.com"
```

Sostituisci *example.com* nell'esempio precedente con l'identità per la quale desideri ottenere i registri DKIM. Puoi specificare un indirizzo e-mail o un dominio.

2. L'output di questo comando contiene una sezione `DkimTokens`, come nell'esempio seguente:

```
{
    "DkimAttributes": {
        "example.com": {
            "DkimEnabled": true,
            "DkimVerificationStatus": "Success",
            "DkimTokens": [
                "hirjd4exampled5477y22yd23ettobi",
                "v3rnz522czcl46quexamplek3efo5o6x",
                "y4examplexbhyhnsjcmtvzotfvqjmdqoj"
            ]
        }
    }
}
```

Puoi utilizzare i token per creare i record CNAME aggiunti alle impostazioni DNS per il tuo dominio. Per creare i record CNAME, utilizza il seguente modello:

```
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
```

Sostituisci ogni istanza di *token1* con il primo token nell'elenco che hai ricevuto quando hai eseguito il comando `get-identity-dkim-attributes`, sostituisci tutte le istanze di *token2* con il secondo token nell'elenco e sostituisci tutte le istanze di *token3* con il terzo token nell'elenco.

Ad esempio, applicando questo modello ai token mostrati nell'esempio precedente otterrai i seguenti record:

```
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**
>
> Se hai selezionato Regione AWS Città del Capo, Osaka o Milano, dovrai utilizzare domini DKIM specifici della regione, come specificato nella tabella Domini DKIM disponibile in. Riferimenti generali di AWS

Disabilitazione di Easy DKIM per un'identità

Puoi disabilitare in modo rapido l'autenticazione DKIM per un'identità utilizzando la console Amazon SES.

Disabilitazione di DKIM per un'identità

1. Accedi AWS Management Console e apri la console Amazon SES all'indirizzo https://console.aws.amazon.com/ses/.
2. Nel pannello di navigazione, in Configuration (Configurazione), scegli Verified identities (Identità verificate).
3. Nell'elenco delle identità, scegli l'identità per la quale desideri disabilitare DKIM.
4. Nella scheda Autenticazione, nel contenitore DomainKeysIdentified Mail (DKIM), scegli Modifica.
5. In Advanced DKIM settings (Impostazioni DKIM avanzate), deseleziona la casella Enabled (Abilitate) nel campo DKIM signatures (Firme DKIM).

Puoi anche disabilitare DKIM per un'identità tramite l'API Amazon SES. Un metodo comune di interazione con l'API è rappresentato dall'utilizzo dell' AWS CLI.

Per disabilitare DKIM per un'identità utilizzando il AWS CLI

- Nella riga di comando, digita il comando seguente:

  ```
  aws ses set-identity-dkim-enabled --identity example.com --no-dkim-enabled
  ```

  Sostituisci *example.com* nell'esempio precedente con l'identità per la quale desideri disabilitare DKIM. Puoi specificare un indirizzo e-mail o un dominio.

Abilitazione di Easy DKIM per un'identità

Se hai già disabilitato DKIM per un'identità, puoi abilitarlo di nuovo tramite la console Amazon SES.

Abilitazione di DKIM per un'identità

1. Accedi AWS Management Console e apri la console Amazon SES all'indirizzo https://console.aws.amazon.com/ses/.
2. Nel pannello di navigazione, in Configuration (Configurazione), scegli Verified identities (Identità verificate).
3. Nell'elenco di identità, scegli l'identità per la quale desideri abilitare DKIM.
4. Nella scheda Autenticazione, nel contenitore DomainKeysIdentified Mail (DKIM), scegli Modifica.
5. In Advanced DKIM settings (Impostazioni avanzate di DKIM), seleziona la casella Enabled (Abilitate) nel campo DKIM signatures (Firme DKIM).

Puoi anche abilitare DKIM per un'identità tramite l'API Amazon SES. Un metodo comune di interazione con l'API è rappresentato dall'utilizzo dell' AWS CLI.

Per abilitare DKIM per un'identità utilizzando il AWS CLI

- Nella riga di comando, digita il comando seguente:

  ```
  aws ses set-identity-dkim-enabled --identity example.com --dkim-enabled
  ```

  Sostituisci *example.com* nell'esempio precedente con l'identità per la quale desideri abilitare DKIM. Puoi specificare un indirizzo e-mail o un dominio.

Sovrascrittura della firma DKIM ereditata su un'identità di indirizzo e-mail

Questa sezione illustra come sovrascrivere (disabilitare o abilitare) le proprietà della firma DKIM ereditate dal dominio padre su un'identità di indirizzo e-mail specifica che hai già verificato con Amazon SES. Puoi eseguire questa operazione solo per le identità degli indirizzi e-mail appartenenti a domini già di tua proprietà, perché le impostazioni DNS sono configurate a livello di dominio.

> **Important**
>
> Non puoi disabilitare/abilitare la firma DKIM per le identità degli indirizzi e-mail…

- su domini che non sono di tua proprietà; Ad esempio, non puoi impostare la firma DKIM per un indirizzo gmail.com o hotmail.com
- su domini di tua proprietà, ma che non sono ancora stati verificati in Amazon SES;
- su domini di tua proprietà, ma su cui non hai abilitato la firma DKIM.

Questa sezione contiene i seguenti argomenti:

- Informazioni sulle proprietà della firma DKIM ereditate
- Sovrascrittura della firma DKIM sull'identità di un indirizzo e-mail (console)
- Sovrascrittura della firma DKIM su un'identità di indirizzo e-mail (AWS CLI)

Informazioni sulle proprietà della firma DKIM ereditate

È importante comprendere innanzitutto che un'identità di indirizzo e-mail eredita le proprietà della firma DKIM dal proprio dominio padre se quest'ultimo è stato configurato con DKIM, indipendentemente dal fatto che sia stato utilizzato Easy DKIM o BYODKIM. Pertanto, la disabilitazione o l'abilitazione della firma DKIM sull'identità dell'indirizzo e-mail, in effetti, sovrascrive le proprietà della firma DKIM del dominio in base a questi fattori chiave:

- Se hai già configurato DKIM per il dominio a cui appartiene l'indirizzo e-mail, non è necessario abilitare la firma DKIM anche per l'identità dell'indirizzo e-mail.
  - Quando configuri DKIM per un dominio, Amazon SES esegue automaticamente l'autenticazione di ogni e-mail da ogni indirizzo di tale dominio, attraverso le proprietà DKIM ereditate per il dominio padre.
- Le impostazioni DKIM per un'identità di indirizzo e-mail specifica sovrascrivono automaticamente le impostazioni del dominio padre o del sottodominio (se applicabile) cui l'indirizzo appartiene.

Poiché le proprietà della firma DKIM dell'identità dell'indirizzo e-mail vengono ereditate dal dominio padre, se prevedi di sovrascriverle, devi tenere presente le regole gerarchiche di sovrascrittura, come spiegato nella tabella seguente.

Firma DKIM disabilitata per il dominio padre	Il dominio padre ha la firma DKIM abilitata
Non è possibile abilitare la firma di DKIM sull'identità dell'indirizzo e-mail.	Puoi disabilitare la firma di DKIM sull'identità dell'indirizzo e-mail.
	Puoi abilitare nuovamente la firma DKIM sull'identità dell'indirizzo e-mail.

In genere non è consigliabile disabilitare la firma DKIM, in quanto rischia di compromettere la reputazione del mittente e aumenta il rischio che la posta inviata venga trasferita nelle cartelle della posta indesiderata o dello spam o che il dominio venga falsificato.

Tuttavia, esiste la possibilità di sovrascrivere le proprietà della firma DKIM ereditate dal dominio sull'identità di un indirizzo e-mail per eventuali casi d'uso particolari o decisioni aziendali esterne per cui sia necessario disabilitare in modo permanente o temporaneo la firma DKIM o abilitarla nuovamente in un secondo momento.

Sovrascrittura della firma DKIM sull'identità di un indirizzo e-mail (console)

La seguente procedura della console SES illustra come sovrascrivere (disabilitare o abilitare) le proprietà della firma DKIM ereditate dal dominio padre sull'identità di un indirizzo e-mail specifico che hai già verificato con Amazon SES.

Disabilitazione/abilitazione della firma DKIM per l'identità di un indirizzo e-mail utilizzando la console

1. Accedi AWS Management Console e apri la console Amazon SES all'indirizzo https://console.aws.amazon.com/ses/.
2. Nel pannello di navigazione, in Configuration (Configurazione), scegli Verified identities (Identità verificate).
3. Nell'elenco di identità scegli un'identità in cui l'opzione Identity type (Tipo di identità) è Email address (Indirizzo e-mail) e appartiene a uno dei tuoi domini verificati.
4. Nella scheda Autenticazione, nel contenitore DomainKeys Identified Mail (DKIM), scegli Modifica.

> **Note**
>
> La scheda Authentication (Autenticazione) è presente solo se l'identità dell'indirizzo e-mail selezionato appartiene a un dominio che è già stato verificato da SES. Se non hai ancora verificato il tuo dominio, consulta Creazione di un'identità dominio.

5. In Advanced DKIM settings (Impostazioni avanzate di DKIM), nel campo DKIM signatures (Firme DKIM), deseleziona la casella di controllo Enabled (Abilitata) per disabilitare la firma DKIM o selezionarla per riabilitare la firma DKIM (se era stata sovrascritta in precedenza).
6. Seleziona Salvataggio delle modifiche.

Sovrascrittura della firma DKIM su un'identità di indirizzo e-mail (AWS CLI)

L'esempio seguente utilizza il comando e AWS CLI i parametri dell'API SES che sostituiranno (disabiliteranno o abiliteranno) le proprietà di firma DKIM ereditate dal dominio principale su un'identità di indirizzo e-mail specifica che hai già verificato con SES.

Per disabilitare/abilitare la firma DKIM per un'identità di indirizzo e-mail utilizzando la AWS CLI

- Ipotizzando che tu possieda il dominio example.com e desideri disabilitare la firma DKIM per uno degli indirizzi e-mail del dominio, digita il comando seguente nella riga di comando:

```
aws sesv2 put-email-identity-dkim-attributes --email-identity marketing@example.com
 --no-signing-enabled
```

  a. Sostituisci *marketing@example.com* con l'identità dell'indirizzo e-mail per la quale desideri disabilitare la firma DKIM.

  b. `--no-signing-enabled` disabilita la firma DKIM. Per riabilitare la firma DKIM, utilizza il comando `--signing-enabled`.

Firma DKIM manuale in Amazon SES

In alternativa all'utilizzo di Easy DKIM, puoi aggiungere manualmente firme DKIM per i tuoi messaggi e quindi inviare i messaggi utilizzando Amazon SES. Se scegli di firmare manualmente i tuoi messaggi, devi prima creare una firma DKIM. Dopo aver creato il messaggio e la firma DKIM, puoi utilizzare l'API SendRawEmail per effettuare l'invio.

Se decidi di firmare manualmente la tua e-mail, considera i seguenti fattori:

- Ogni messaggio inviato utilizzando Amazon SES contiene un'intestazione DKIM che fa riferimento a un dominio di firma di amazonses.com, il quale contiene la seguente stringa: `d=amazonses.com`. Se firmi manualmente i tuoi messaggi, tali messaggi dovranno includere due intestazioni DKIM: una per il tuo dominio e una che Amazon SES crea automaticamente per amazonses.com.
- Amazon SES non convalida le firme DKIM aggiunte manualmente ai tuoi messaggi. In caso di errori con la firma DKIM in un messaggio, il medesimo potrebbe essere rifiutato dal provider di posta elettronica.
- Quando firmi i tuoi messaggi, ti consigliamo di utilizzare una lunghezza di almeno 1024 bit.
- Non firmare i seguenti campi: ID messaggio, Data, Percorso di ritorno, Rinvia a.

> **Note**
>
> Se utilizzi un client e-mail per l'invio di e-mail utilizzando l'interfaccia SMTP Amazon SES, il client potrebbe eseguire automaticamente la firma DKIM dei tuoi messaggi. Alcuni client potrebbero firmare solo alcuni di questi campi. Consulta la documentazione relativa al tuo client e-mail per verificare quali campi vengono firmati per impostazione predefinita.

Autenticazione delle e-mail con SPF in Amazon SES

Sender Policy Framework (SPF) è uno standard di convalida di e-mail, progettato per combattere lo spoofing delle e-mail. I proprietari di dominio utilizzano SPF per indicare ai provider di posta elettronica quali server sono autorizzati a inviare e-mail dai propri domini. SPF è definito in RFC 7208.

Per impostazione predefinita, i messaggi inviati tramite Amazon SES usano un dominio secondario di `amazonses.com` come dominio MAIL FROM. L'autenticazione di SPF (Sender Policy Framework) permette di convalidare correttamente questi messaggi perché il dominio MAIL FROM predefinito corrisponde al server di invio della posta, in questo caso SES. Pertanto, in SES, SPF è configurato implicitamente per te.

Tuttavia, se non si desidera utilizzare il dominio MAIL FROM predefinito di SES e si preferisce utilizzare un sottodominio di un dominio di propria proprietà, in SES si parla di un dominio MAIL FROM personalizzato. Per fare ciò, è necessario pubblicare il proprio record SPF per il dominio MAIL FROM personalizzato. Inoltre, SES richiede la pubblicazione di un record MX in modo che il tuo

dominio MAIL FROM personalizzato possa ricevere le notifiche di mancato recapito e reclamo inviate dai provider di posta elettronica.

Scopri come configurare l'autenticazione SPF

Vengono fornite istruzioni per configurare il dominio con SPF e come pubblicare i record MX e SPF (tipo TXT) in. the section called “Uso di un dominio MAIL FROM personalizzato”

Uso di un dominio MAIL FROM personalizzato

Quando un'e-mail viene inviata, ha due indirizzi che ne indicano l'origine: un indirizzo From (Da) visualizzato al destinatario del messaggio e un indirizzo MAIL FROM che indica l'origine del messaggio. L'indirizzo MAIL FROM a volte viene chiamato indirizzo mittente busta, mittente da, indirizzo di mancato recapito o indirizzo percorso di ritorno. I server di posta utilizzano l'indirizzo MAIL FROM per restituire messaggi di mancato recapito e altre notifiche di errore. L'indirizzo MAIL FROM è in genere visibile solo dai destinatari se visualizzano il codice sorgente per il messaggio.

Amazon SES imposta il dominio MAIL FROM per i messaggi inviati a un valore predefinito a meno che non specifichi il tuo dominio (personalizzato). Questa sezione illustra i vantaggi della configurazione di un dominio MAIL FROM personalizzato e include le procedure di configurazione.

Perché usare un dominio MAIL FROM personalizzato?

Per impostazione predefinita, i messaggi inviati tramite Amazon SES usano un dominio secondario di `amazonses.com` come dominio MAIL FROM. L'autenticazione SPF (Sender Policy Framework) permette di convalidare correttamente questi messaggi perché il dominio MAIL FROM predefinito corrisponde al server di invio della posta, in questo caso SES.

Se non si desidera utilizzare il dominio SES MAIL FROM predefinito e si preferisce utilizzare un sottodominio di un dominio di proprietà, in SES si parla di utilizzo di un dominio MAIL FROM personalizzato. Per fare ciò, è necessario pubblicare il proprio record SPF per il dominio MAIL FROM personalizzato. Inoltre, sES richiede anche la pubblicazione di un record MX in modo che il tuo dominio possa ricevere le notifiche di mancato recapito e reclamo inviate dai provider di posta elettronica.

Utilizzando un dominio MAIL FROM personalizzato, hai la flessibilità di utilizzare SPF, DKIM o entrambi per ottenere la convalida DMARC (Domain-based Message Authentication, Reporting and Conformance). DMARC consente al dominio di un mittente di indicare che le e-mail inviate dal dominio sono protette da uno o più sistemi di autenticazione. Ci sono due modi per ottenere

la convalida DMARC: the section called “Conformità a DMARC tramite SPF” e the section called “Conformità a DMARC tramite DKIM”.

Scelta di un dominio MAIL FROM personalizzato

Di seguito, il termine dominio MAIL FROM si riferisce sempre a un sottodominio di un dominio di tua proprietà: questo sottodominio che usi per il tuo dominio MAIL FROM personalizzato non deve essere utilizzato per nient'altro e soddisfa i seguenti requisiti:

- Il dominio MAIL FROM deve essere un sottodominio del dominio principale di un'identità verificata (indirizzo email o dominio).
- Il dominio MAIL FROM non deve essere un dominio secondario da cui si inviano e-mail.
- Il dominio MAIL FROM non deve essere un dominio secondario usato per ricevere e-mail.

Uso di SPF con un dominio MAIL FROM personalizzato

Sender Policy Framework (SPF) è uno standard di convalida di e-mail, progettato per combattere lo spoofing delle e-mail. È possibile configurare il dominio MAIL FROM personalizzato con SPF per indicare ai provider di posta elettronica quali server sono autorizzati a inviare e-mail dal dominio MAIL FROM personalizzato. SPF è definito in RFC 7208.

Per configurare un registro SPF, è necessario pubblicare un nuovo record TXT alla configurazione DNS per il dominio MAIL FROM personalizzato. Questo registro contiene un elenco dei server autorizzati a inviare messaggi di posta elettronica dal dominio MAIL FROM personalizzato. Quando un provider di posta elettronica riceve un messaggio dal dominio MAIL FROM, controlla i record DNS per il dominio per verificare che l'e-mail sia stata inviata da un server autorizzato.

Se si desidera utilizzare questo record SPF per conformarsi a DMARC, il dominio nell'indirizzo From deve corrispondere al dominio MAIL FROM. Per informazioni, consulta the section called “Conformità a DMARC tramite SPF”.

La prossima sezione, the section called “Configurazione del dominio MAIL FROM personalizzato”, spiega come configurare SPF per il tuo dominio MAIL FROM personalizzato.

Configurazione del dominio MAIL FROM personalizzato

Il processo di configurazione di un dominio MAIL FROM personalizzato richiede di aggiungere record alla configurazione DNS per il dominio. SES richiede la pubblicazione di un record MX in modo che il dominio possa ricevere le notifiche di rimbalzo e di reclamo inviate dai provider di posta elettronica.

Devi inoltre pubblicare un record SPF (tipo TXT) per dimostrare che Amazon SES è autorizzato a inviare e-mail dal tuo dominio.

È possibile configurare un dominio MAIL FROM personalizzato per un intero dominio o sottodominio, nonché per singoli indirizzi e-mail. Le procedure seguenti mostrano come utilizzare la console Amazon SES per configurare un dominio MAIL FROM personalizzato. Puoi anche configurare un dominio MAIL FROM personalizzato utilizzando l'operazione SetIdentityMailFromDomain API.

Configurazione di un dominio MAIL FROM personalizzato per un dominio verificato

Queste procedure mostrano come configurare un dominio MAIL FROM personalizzato per un intero dominio o sottodominio in modo che tutti i messaggi inviati dagli indirizzi di quel dominio utilizzino questo dominio MAIL FROM personalizzato.

Per configurare un dominio verificato per utilizzare un dominio MAIL FROM personalizzato specificato

1. Aprire la console Amazon SES all'indirizzo https://console.aws.amazon.com/ses/.
2. Nel pannello di navigazione a sinistra, in Configurazione, scegli Identità.
3. Nell'elenco delle identità, scegli quella da configurare che abbia queste caratteristiche: Identity type (Tipo di identità) corrisponde a Domain (Dominio) e Status (Stato) corrisponde a Verified (Verificato).
    - Se Status (Stato) corrisponde a Unverified (Non verificato), completa le procedure indicate in Verifica dell'identità di un dominio DKIM con il provider DNS per verificare il dominio dell'indirizzo e-mail.
4. Nella parte inferiore della schermata nel riquadro Custom MAIL FROM domain (Dominio MAIL FROM personalizzato), scegli Edit (Modifica).
5. Nel riquadro General details (Dettagli generali), procedi come segue:
    a. Seleziona la casella di controllo Use a custom MAIL FROM domain (Utilizza dominio MAIL FROM personalizzato).
    b. Per MAIL FROM domain (Dominio MAIL FROM), immetti il dominio secondario che desideri utilizzare come dominio MAIL FROM.
    c. Per Behavior on MX failure (Comportamento con errore MX), scegli una delle opzioni seguenti:
        - Use default MAIL FROM domain (Usa dominio MAIL FROM di default): se il registro MX del dominio MAIL FROM personalizzato non è configurato correttamente, Amazon SES

usa un sottodominio di `amazonses.com`. Il sottodominio varia in base al tipo Regione AWS di utilizzo di Amazon SES.

- Reject message (Rifiuta messaggio): se il record MX del dominio MAIL FROM personalizzato non è configurato correttamente, Amazon SES restituisce un errore `MailFromDomainNotVerified`. I messaggi e-mail che tenti di inviare da questo dominio verranno automaticamente rifiutati.

d. Scegli Save changes (Salva le modifiche): verrai riportato alla schermata precedente.

6. Pubblica i record MX ed SFP (tipo TXT) nel server DNS del dominio MAIL FROM personalizzato:

Nel riquadro Custom MAIL FROM domain (Dominio MAIL FROM personalizzato), la tabella Publish DNS records (Pubblicazione di record DNS) ora visualizza i record MX ed SPF (tipo TXT) in quelli da pubblicare (aggiungere) alla configurazione DNS del dominio. Questi record utilizzano i formati mostrati nella tabella seguente.

Nome	Type	Valore
dominio secondario .*dominio.com*	MX	10 feedback-smtp.*Regione*.amazonses.com
dominio secondario .*dominio.com*	TXT	"v=spf1 include:amazonses.com ~all"

Nei record precedenti,

- *sottodominio*.*dominio*.*com* verrà popolato con il sottodominio MAIL FROM
- la *regione* verrà popolata con il nome del dominio MAIL FROM Regione AWS in cui desideri verificare (ad esempious-west-2, o us-east-1eu-west-1, ecc.)
- Il numero 10 elencato insieme al valore MX è l'ordine di preferenza per il server di posta elettronica e dovrà essere inserito in un campo valore separato come specificato dalla GUI del provider DNS
- Il valore del record TXT di SFP deve includere le virgolette

Dalla tabella Publish DNS records (Pubblicazione di record DNS), copia i record MX e SPF (tipo TXT) scegliendo l'icona di copia accanto a ciascun valore e incollali nei campi corrispondenti

nella GUI del provider DNS. In alternativa, puoi scegliere Download .csv record set (Scarica il set di record .csv) per salvare una copia dei record sul tuo computer.

> **Important**
>
> Per configurare correttamente un dominio MAIL FROM con Amazon SES, è necessario pubblicare esattamente un registro MX nel server DNS del dominio MAIL FROM. Se il dominio MAIL FROM contiene più registri MX, l'impostazione del dominio MAIL FROM personalizzato con Amazon SES non riesce.

Se Route 53 fornisce il servizio DNS per il tuo dominio MAIL FROM e hai effettuato l'accesso AWS Management Console con lo stesso account che usi per Route 53, scegli Pubblica record utilizzando Route 53. I record DNS vengono applicati automaticamente alla configurazione DNS del dominio.

Se utilizzi un provider DNS diverso, pubblica i record DNS nel server DNS del dominio MAIL FROM manualmente. La procedura per aggiungere record DNS al server DNS del dominio varia in base al servizio di hosting Web o al provider DNS.

Le procedure per la pubblicazione dei record DNS dei domini variano a seconda del provider DNS. La tabella che segue include i collegamenti alla documentazione dei provider DNS più comunemente utilizzati. Questo elenco non è esaustivo e non significa approvazione; allo stesso modo, se il provider DNS non è elencato, non implica che non supporti la configurazione del dominio MAIL FROM.

Nome del provider di DNS/Hosting	Collegamento alla documentazione
GoDaddy	• MX: Aggiunta di un record (collegamento esterno) • TXT: Aggiunta di un record TXT (collegamento esterno)
DreamHost	• MX: Come modificare i miei record MX? (collegamento esterno) • TXT: Come aggiungere record DNS personalizzati? (collegamento esterno)

Nome del provider di DNS/Hosting	Collegamento alla documentazione
Cloudflare	• MX: Come aggiungere o modificare record e-mail o MX? (collegamento esterno) • TXT: Gestione di record DNS in CloudFlare (collegamento esterno)
HostGator	• MX: onfigurazione dei record MX (link esterno) • TXT: gestisci i record DNS con HostGator / eNom (link esterno)
Namecheap	• MX: Come posso configurare i record MX richiesti per il servizio di posta elettronica? (collegamento esterno) • TXT: Come aggiungo i record TXT/SPF/DKIM/DMARC per il mio dominio? (collegamento esterno)
Names.co.uk	• MX: Modifica delle impostazioni DNS del dominio (collegamento esterno) • TXT: Modifica delle impostazioni DNS del dominio (collegamento esterno)
Wix	• MX: Aggiunta o aggiornamento di record MX nell'account Wix (collegamento esterno) • TXT: Aggiunta o aggiornamento di record TXT nell'account Wix (collegamento esterno)

Quando Amazon SES rileva che i record sono presenti, riceverai un'e-mail che informa che il tuo dominio MAIL FROM personalizzato è stato configurato correttamente. A seconda del provider DNS, potrebbe esserci un ritardo fino a 72 ore prima che Amazon SES rilevi il registro MX.

Configurazione di un dominio MAIL FROM personalizzato per un indirizzo e-mail verificato

Puoi anche configurare un dominio MAIL FROM personalizzato per un indirizzo e-mail specifico. Per configurare un dominio MAIL FROM personalizzato per un indirizzo e-mail, devi modificare i record DNS per il dominio a cui è associato l'indirizzo e-mail.

> **Note**
>
> Non puoi configurare un dominio MAIL FROM personalizzato per gli indirizzi su un dominio che non sia di tua proprietà (ad esempio, non puoi creare un dominio MAIL FROM personalizzato per un indirizzo sul dominio `gmail.com`, perché non puoi aggiungere i registri DNS necessari al dominio).

Configurazione di un indirizzo e-mail verificato per l'uso di un dominio MAIL FROM specificato

1. Aprire la console Amazon SES all'indirizzo https://console.aws.amazon.com/ses/.
2. Nel pannello di navigazione a sinistra, in Configurazione, scegli Identità.
3. Nell'elenco delle identità, scegli l'identità che desideri configurare, dove Identity type (Tipo di identità) è Email address (Indirizzo e-mail) e Status (Stato) è Verified (Verificato).
   - Se Status (Stato) corrisponde a Unverified (Non verificato), completa i passaggi indicati nella sezione Verifica di un'identità indirizzo e-mail per verificare il dominio dell'indirizzo e-mail.
4. Nella scheda MAIL FROM Domain (Dominio MAIL FROM), scegli Edit (Modifica) nel riquadro Custom MAIL FROM domain (Dominio MAIL FROM personalizzato).
5. Nel riquadro General details (Dettagli generali), procedi come segue:
   a. Seleziona la casella di controllo Use a custom MAIL FROM domain (Utilizza dominio MAIL FROM personalizzato).
   b. Per MAIL FROM domain (Dominio MAIL FROM), immetti il dominio secondario che desideri utilizzare come dominio MAIL FROM.
   c. Per Behavior on MX failure (Comportamento con errore MX), scegli una delle opzioni seguenti:
      - Use default MAIL FROM domain (Usa dominio MAIL FROM di default): se il registro MX del dominio MAIL FROM personalizzato non è configurato correttamente, Amazon SES usa un sottodominio di `amazonses.com`. Il sottodominio varia in base al tipo Regione AWS di utilizzo di Amazon SES.

- Reject message (Rifiuta messaggio): se il record MX del dominio MAIL FROM personalizzato non è configurato correttamente, Amazon SES restituisce un errore `MailFromDomainNotVerified`. I messaggi e-mail che tenti di inviare da questo indirizzo verranno automaticamente rifiutati.

d. Scegli Save changes (Salva le modifiche): verrai riportato alla schermata precedente.

6. Pubblica i record MX ed SFP (tipo TXT) nel server DNS del dominio MAIL FROM personalizzato:

Nel riquadro Custom MAIL FROM domain (Dominio MAIL FROM personalizzato), la tabella Publish DNS records (Pubblicazione di record DNS) ora visualizza i record MX ed SPF (tipo TXT) in quelli da pubblicare (aggiungere) alla configurazione DNS del dominio. Questi record utilizzano i formati mostrati nella tabella seguente.

Nome	Type	Valore
dominio secondario .dominio.com	MX	10 feedback-smtp.*Regione*.amazonses.com
dominio secondario .dominio.com	TXT	"v=spf1 include:amazonses.com ~all"

Nei record precedenti,

- *sottodominio*.*dominio*.*com* verrà popolato con il sottodominio MAIL FROM
- la *regione* verrà popolata con il nome del dominio MAIL FROM Regione AWS in cui desideri verificare (ad esempio`us-west-2`, o `us-east-1eu-west-1`, ecc.)
- Il numero 10 elencato insieme al valore MX è l'ordine di preferenza per il server di posta elettronica e dovrà essere inserito in un campo valore separato come specificato dalla GUI del provider DNS
- Il valore del record TXT di SFP deve includere le virgolette

Dalla tabella Publish DNS records (Pubblicazione di record DNS), copia i record MX e SPF (tipo TXT) scegliendo l'icona di copia accanto a ciascun valore e incollali nei campi corrispondenti nella GUI del provider DNS. In alternativa, puoi scegliere Download .csv record set (Scarica il set di record .csv) per salvare una copia dei record sul tuo computer.

> **Important**
>
> Per configurare correttamente un dominio MAIL FROM con Amazon SES, è necessario pubblicare esattamente un registro MX nel server DNS del dominio MAIL FROM. Se il dominio MAIL FROM contiene più registri MX, l'impostazione del dominio MAIL FROM personalizzato con Amazon SES non riesce.

Se Route 53 fornisce il servizio DNS per il tuo dominio MAIL FROM e hai effettuato l'accesso AWS Management Console con lo stesso account che usi per Route 53, scegli Pubblica record utilizzando Route 53. I record DNS vengono applicati automaticamente alla configurazione DNS del dominio.

Se utilizzi un provider DNS diverso, pubblica i record DNS nel server DNS del dominio MAIL FROM manualmente. La procedura per aggiungere record DNS al server DNS del dominio varia in base al servizio di hosting Web o al provider DNS.

Le procedure per la pubblicazione dei record DNS dei domini variano a seconda del provider DNS. La tabella che segue include i collegamenti alla documentazione dei provider DNS più comunemente utilizzati. Questo elenco non è esaustivo e non significa approvazione; allo stesso modo, se il provider DNS non è elencato, non implica che non supporti la configurazione del dominio MAIL FROM.

Nome del provider di DNS/Hosting	Collegamento alla documentazione
GoDaddy	• MX: Aggiunta di un record (collegamento esterno) • TXT: Aggiunta di un record TXT (collegamento esterno)
DreamHost	• MX: Come modificare i miei record MX? (collegamento esterno) • TXT: Come aggiungere record DNS personalizzati? (collegamento esterno)

Nome del provider di DNS/Hosting	Collegamento alla documentazione
Cloudflare	• MX: Come aggiungere o modificare record e-mail o MX? (collegamento esterno) • TXT: Gestione di record DNS in CloudFlare (collegamento esterno)
HostGator	• MX: Modifica di record MX - Windows (collegamento esterno) • TXT: gestisci i record DNS con HostGator / eNom (link esterno)
Namecheap	• MX: Come posso configurare i record MX richiesti per il servizio di posta elettronica? (collegamento esterno) • TXT: Come aggiungo i record TXT/SPF/DKIM/DMARC per il mio dominio? (collegamento esterno)
Names.co.uk	• MX: Modifica delle impostazioni DNS del dominio (collegamento esterno) • TXT: Modifica delle impostazioni DNS del dominio (collegamento esterno)
Wix	• MX: Aggiunta o aggiornamento di record MX nell'account Wix (collegamento esterno) • TXT: Aggiunta o aggiornamento di record TXT nell'account Wix (collegamento esterno)

Quando Amazon SES rileva che i record sono presenti, riceverai un'e-mail che informa che il tuo dominio MAIL FROM personalizzato è stato configurato correttamente. A seconda del provider DNS, potrebbe esserci un ritardo fino a 72 ore prima che Amazon SES rilevi il registro MX.

Stati di impostazione del dominio MAIL FROM personalizzato con Amazon SES

Dopo aver configurato un'identità per usare un dominio MAIL FROM personalizzato, lo stato dell'impostazione è "pending" (in attesa) mentre Amazon SES tenta di rilevare il registro MX necessario nelle impostazioni DNS. Lo stato quindi cambia a seconda del fatto che Amazon SES rilevi o meno il registro MX. La tabella seguente descrive il comportamento di invio dei messaggi e-mail e le operazioni di Amazon SES associate a ogni stato. Ogni volta che lo stato cambia, Amazon SES invia una notifica all'indirizzo e-mail associato al tuo Account AWS.

Stato	Comportamento di invio di e-mail	Operazioni di Amazon SES
In attesa	Viene usata l'impostazione di fallback del dominio MAIL FROM personalizzato	Amazon SES tenta di rilevare il registro MX necessario per 72 ore. Se l'operazione non riesce, lo stato diventa "Failed" (Non riuscito).
Riuscito	Viene usato il dominio MAIL FROM personalizzato	Amazon SES controlla continuamente che il record MX necessario sia disponibile.
Temporary Failure	Viene usata l'impostazione di fallback del dominio MAIL FROM personalizzato	Amazon SES tenta di rilevare il registro MX necessario per 72 ore. In caso di esito negativo, lo stato diventa "Failed" (Non

Stato	Comportamento di invio di e-mail	Operazioni di Amazon SES
		riuscito), mentre in caso di esito positivo lo stato cambia in "Success" (Riuscito).
Non riuscito	Viene usata l'impostazione di fallback del dominio MAIL FROM personalizzato	Amazon SES non tenta più di rilevare il record MX necessario. Per usare un dominio MAIL FROM personalizzato, è necessario riavviare il processo di impostazione in Configurazione del dominio MAIL FROM personalizzato.

Conformità al protocollo di autenticazione DMARC in Amazon SES

DMARC (Domain-based Message Authentication, Reporting and Conformance) è un protocollo di autenticazione e-mail che utilizza Sender Policy Framework (SPF) e DomainKeys Identified Mail (DKIM) per rilevare lo spoofing e il phishing delle e-mail. Per essere conformi a DMARC, i messaggi devono essere autenticati tramite SPF o DKIM, ma idealmente, quando entrambi vengono utilizzati con DMARC, garantirete il massimo livello di protezione possibile per l'invio di e-mail.

Esaminiamo brevemente cosa fa ciascuno di essi e come DMARC li collega tutti insieme:

- SPF — Identifica quali server di posta sono autorizzati a inviare posta per conto del dominio MAIL FROM personalizzato tramite un record DNS TXT utilizzato dal DNS. I sistemi di posta dei destinatari fanno riferimento al record TXT SPF per determinare se un messaggio proveniente dal dominio personalizzato proviene da un server di messaggistica autorizzato. Fondamentalmente, SPF è progettato per aiutare a prevenire lo spoofing, ma esistono tecniche di spoofing a cui SPF è suscettibile nella pratica ed è per questo che è necessario utilizzare anche DKIM insieme a DMARC.
- DKIM: aggiunge una firma digitale ai messaggi in uscita nell'intestazione dell'e-mail. I sistemi di ricezione delle e-mail possono utilizzare questa firma digitale per verificare se le e-mail in arrivo sono firmate da una chiave di proprietà del dominio. Tuttavia, quando un sistema di posta elettronica ricevente inoltra un messaggio, la busta del messaggio viene modificata in modo da invalidare l'autenticazione SPF. Poiché la firma digitale rimane nel messaggio di posta elettronica perché fa parte dell'intestazione dell'e-mail, DKIM funziona anche quando un messaggio è stato inoltrato tra server di posta (purché il contenuto del messaggio non sia stato modificato).
- DMARC: assicura l'allineamento del dominio con almeno uno tra SPF e DKIM. L'uso di SPF e DKIM da soli non fa nulla per assicurare che l'indirizzo From sia autenticato (questo è l'indirizzo e-mail che il destinatario vede nel suo client di posta elettronica). SPF controlla solo il dominio specificato nell'indirizzo MAIL FROM (non visualizzato dal destinatario). DKIM controlla solo il dominio specificato nella firma DKIM (inoltre, non viene visualizzato dal destinatario). DMARC risolve questi due problemi richiedendo che l'allineamento del dominio sia corretto su SPF o DKIM:
  - Affinché SPF passi l'allineamento DMARC, il dominio nell'indirizzo From deve corrispondere al dominio nell'indirizzo MAIL FROM (noto anche come indirizzo Return-Path e Envelope-from). Ciò è raramente possibile con la posta inoltrata perché viene rimossa o quando si invia posta tramite provider di posta elettronica di massa di terze parti, perché il Return-Path (MAIL FROM) viene utilizzato per rimbalzi e reclami che il provider (SES) monitora utilizzando un indirizzo di sua proprietà.
  - Affinché DKIM passi l'allineamento DMARC, il dominio specificato nella firma DKIM deve corrispondere al dominio nell'indirizzo From. Se utilizzi mittenti o servizi di terze parti che inviano posta per tuo conto, puoi farlo assicurandoti che il mittente terzo sia configurato correttamente per la firma DKIM e che tu abbia aggiunto i record DNS appropriati all'interno del tuo dominio. I server di posta riceventi saranno quindi in grado di verificare le e-mail inviate loro da terze parti come se fossero e-mail inviate da qualcuno autorizzato a utilizzare un indirizzo all'interno del dominio.

Mettendo tutto insieme con DMARC

I controlli di allineamento DMARC di cui abbiamo parlato sopra mostrano come SPF, DKIM e DMARC collaborino per aumentare la fiducia del dominio e la consegna delle e-mail nelle caselle di posta. DMARC ottiene ciò assicurando che l'indirizzo From, visto dal destinatario, sia autenticato da SPF o DKIM:

- Un messaggio passa DMARC se uno o entrambi i controlli SPF o DKIM descritti vengono superati.
- Un messaggio non supera il protocollo DMARC se entrambi i controlli SPF o DKIM descritti falliscono.

Pertanto, sia SPF che DKIM sono necessari affinché DMARC abbia le migliori possibilità di ottenere l'autenticazione per le e-mail inviate e, utilizzandoli tutti e tre, contribuirete a garantire un dominio di invio completamente protetto.

DMARC consente inoltre di istruire i server di posta elettronica su come gestire le e-mail quando falliscono l'autenticazione DMARC attraverso le politiche impostate. Questo verrà spiegato nella sezione seguentethe section called “Impostazione della policy DMARC sul tuo dominio”, che contiene informazioni su come configurare i domini SES in modo che le e-mail inviate siano conformi al protocollo di autenticazione DMARC tramite SPF e DKIM.

Impostazione della policy DMARC sul tuo dominio

Per configurare DMARC, devi modificare le impostazioni DNS per il tuo dominio. Le impostazioni DNS per il tuo dominio devono includere un record TXT specificante le impostazioni DMARC del dominio. Le procedure per l'aggiunta di record TXT per la tua configurazione DNS dipendono dal provider di hosting o DNS utilizzato. Se utilizzi Amazon Route 53 per DNS, consulta la sezione Utilizzo dei record nella Guida per gli sviluppatori di Amazon Route 53. Se utilizzi un altro provider, consulta la documentazione del provider relativa alla configurazione DNS.

Il nome del record TXT creato deve essere `_dmarc.`*`example.com`*, in cui *`example.com`* rappresenta il tuo dominio. Il valore del record TXT contiene la policy DMARC che si applica al tuo dominio. Di seguito è riportato un esempio di record TXT contenente una policy DMARC:

Nome	Type	Valore
`_dmarc.example.com`	`TXT`	`"v=DMARC1;p=quarantine;rua=mailto:my_dmarc_report@example.com"`

Nel precedente esempio di politica DMARC, questa politica indica ai provider di posta elettronica di fare quanto segue:

- Per tutti i messaggi che falliscono l'autenticazione, inviateli alla cartella Spam come specificato dal parametro policy,. `p=quarantine` Altre opzioni includono non fare nulla utilizzando `p=none` o rifiutare completamente il messaggio utilizzando. `p=reject`
  - La sezione successiva illustra come e quando utilizzare queste tre impostazioni dei criteri: l'utilizzo di quella sbagliata nel momento sbagliato può causare il mancato recapito delle e-mail, vedi. the section called “Implementazione di DMARC”
- Invia report su tutte le e-mail che non sono riuscite ad autenticarsi in un digest (ovvero un rapporto che aggrega i dati per un determinato periodo di tempo, anziché inviare report individuali per ogni evento) come specificato dal parametro di reporting `rua=mailto:my_dmarc_report@example.com` (rua sta per Reporting URI for Aggregate reports). I provider di posta elettronica in genere inviano questi report aggregati una volta al giorno, anche se tali policy possono variano per ogni provider.

Per ulteriori informazioni sulla configurazione DMARC per il tuo dominio, consulta la Panoramica sul sito Web DMARC.

Per le specifiche complete del sistema DMARC, vedere la bozza DMARC della Internet Engineering Task Force (IETF).

Le migliori pratiche per l'implementazione di DMARC

È meglio implementare l'applicazione della politica DMARC con un approccio graduale e graduale in modo da non interrompere il resto del flusso di posta. Crea e implementa un piano di implementazione che segua questi passaggi. Esegui ciascuno di questi passaggi prima con ciascuno dei tuoi sottodomini e infine con il dominio di primo livello dell'organizzazione prima di passare alla fase successiva.

1. Monitora l'impatto dell'implementazione di DMARC (p=none).
   - Inizia con un semplice record in modalità di monitoraggio per un sottodominio o dominio che richiede che le organizzazioni che ricevono la posta ti inviino statistiche sui messaggi che vedono utilizzando quel dominio. Un record in modalità di monitoraggio è un record DMARC TXT il cui criterio è impostato su none. `p=none`
   - I report generati tramite DMARC forniranno i numeri e le fonti dei messaggi che superano questi controlli, rispetto a quelli che non lo fanno. Puoi facilmente vedere quanto del tuo traffico

legittimo è coperto o meno da essi. Vedrai segni di inoltro, poiché i messaggi inoltrati non rispetteranno gli standard SPF e DKIM se il contenuto viene modificato. Inizierai anche a vedere quanti messaggi fraudolenti vengono inviati e da dove vengono inviati.

- Gli obiettivi di questo passaggio sono capire quali saranno le email che subiranno l'implementazione di uno dei due passaggi successivi e fare in modo che eventuali mittenti terzi o autorizzati allineino le proprie politiche SPF o DKIM.
- Ideale per i domini esistenti.

2. Richiedete che i sistemi di posta esterni mettano in quarantena la posta che non rispetta DMARC (p=quarantine).
   - Se ritieni che tutto o la maggior parte del tuo traffico legittimo provenga da un dominio allineato a SPF o DKIM e comprendi l'impatto dell'implementazione di DMARC, puoi implementare una politica di quarantena. Una politica di quarantena è un record DMARC TXT il cui criterio è impostato sulla quarantena. `p=quarantine` In questo modo, chiedete ai ricevitori DMARC di inserire i messaggi del vostro dominio che non contengono DMARC nell'equivalente locale di una cartella spam anziché nelle caselle di posta dei vostri clienti.
   - Ideale per i domini in transizione che hanno analizzato i report DMARC durante la Fase 1.
3. Richiedete che i sistemi di posta esterni non accettino messaggi che non rispettano il DMARC (p=reject).
   - L'implementazione di una politica di rifiuto è di solito il passaggio finale. Una politica di rifiuto è un record TXT DMARC la cui politica è impostata per rifiutare. `p=reject` Quando lo fai, chiedi ai ricevitori DMARC di non accettare messaggi che non superano i controlli DMARC: questo significa che non verranno nemmeno messi in quarantena in una cartella spam o posta indesiderata, ma verranno respinti a titolo definitivo.
   - Quando si utilizza una politica di rifiuto, saprete esattamente quali messaggi non rispettano la politica DMARC, poiché il rifiuto comporterà un rimbalzo SMTP. Con la quarantena, i dati aggregati forniscono informazioni sulle percentuali di email che superano o non superano i controlli SPF, DKIM e DMARC.
   - Ideale per i nuovi domini o per i domini esistenti che hanno superato i due passaggi precedenti.

Conformità a DMARC tramite SPF

Affinché un'e-mail sia conforme a DMARC in base a SPF, è necessario soddisfare le condizioni seguenti:

- Il messaggio deve superare un controllo SPF basato sulla presenza di un record SPF (tipo TXT) valido da pubblicare nella configurazione DNS del dominio MAIL FROM personalizzato.
- Il dominio nell'indirizzo From dell'intestazione dell'email deve essere allineato (corrispondere) al dominio o a un sottodominio di, specificato nell'indirizzo MAIL FROM. Per ottenere l'allineamento SPF con SES, la politica DMARC del dominio non deve specificare una politica SPF rigorosa (aspf=s).

Per rispettare questi requisiti, completa le fasi seguenti:

- Configura un dominio MAIL FROM personalizzato completando le procedure in the section called "Uso di un dominio MAIL FROM personalizzato".
- Assicurati che il dominio mittente usi una policy flessibile per SPF. Se non hai modificato l'allineamento delle politiche del tuo dominio, per impostazione predefinita utilizza una politica semplificata, così come SES.

> **Note**
>
> Puoi determinare l'allineamento DMARC del dominio per SPF digitando il comando seguente nella riga di comando, sostituendo *example.com* con il tuo dominio:
>
> ```
> dig -type=TXT _dmarc.example.com
> ```
>
> Nell'output del comando, in Non-authoritative answer (Risposta non autorevole) cerca un record che inizia con `v=DMARC1`. Se il record include la stringa `aspf=r` oppure se la stringa `aspf` non è presente, il dominio usa l'allineamento flessibile per SPF. Se il record include la stringa `aspf=s`, il dominio usa l'allineamento rigoroso per SPF. L'amministratore di sistema dovrà rimuovere questo tag dal record TXT DMARC nella configurazione DNS del dominio.
> In alternativa, puoi utilizzare uno strumento di ricerca DMARC basato sul web, come DMARC Inspector dal sito dmarcian o lo strumento DMARC Check Tool dal sito Web, per determinare l'allineamento delle politiche del tuo dominio per SPF. MxToolBox

Conformità a DMARC tramite DKIM

Affinché un'e-mail sia conforme a DMARC in base a DKIM, è necessario soddisfare le condizioni seguenti:

- Il messaggio deve avere una firma DKIM valida e superare il controllo DKIM.
- Il dominio specificato nella firma DKIM deve essere allineato (corrispondere) al dominio nell'indirizzo From. Se la politica DMARC del dominio specifica un allineamento rigoroso per DKIM, questi domini devono corrispondere esattamente (SES utilizza una politica DKIM rigorosa per impostazione predefinita).

Per rispettare questi requisiti, completa le fasi seguenti:

- Configura Easy DKIM completando le procedure in the section called “Easy DKIM”. Quando usi Easy DKIM, Amazon SES firma automaticamente le e-mail.

> **Note**
>
> Se non vuoi usare Easy DKIM, puoi anche firmare manualmente i messaggi. Se scegli di farlo, fai tuttavia molta attenzione, perché Amazon SES non convalida la firma DKIM creata. Per questo motivo, consigliamo di usare Easy DKIM.

- Assicurati che il dominio specificato nella firma DKIM sia allineato al dominio nell'indirizzo From. Oppure, se invii da un sottodominio del dominio nell'indirizzo From, assicurati che la tua politica DMARC sia impostata su un allineamento rilassato.

> **Note**
>
> Puoi determinare l'allineamento DMARC del dominio per DKIM digitando il comando seguente nella riga di comando, sostituendo *example.com* con il tuo dominio:
>
> ```
> dig -type=TXT _dmarc.example.com
> ```
>
> Nell'output del comando, in Non-authoritative answer (Risposta non autorevole) cerca un record che inizia con `v=DMARC1`. Se il record include la stringa `adkim=r` oppure se la stringa `adkim` non è presente, il dominio usa l'allineamento flessibile per DKIM. Se il record include la stringa `adkim=s`, il dominio usa l'allineamento rigoroso per DKIM. L'amministratore di sistema dovrà rimuovere questo tag dal record TXT DMARC nella configurazione DNS del dominio.
> In alternativa, puoi utilizzare uno strumento di ricerca DMARC basato sul web, come DMARC Inspector dal sito dmarcian o lo strumento DMARC Check Tool dal sito Web, per determinare l'allineamento delle politiche del tuo dominio per DKIM. MxToolBox

Utilizzo di BIMI in Amazon SES

Brand Indicators for Message Identification (BIMI) è una specifica e-mail che consente alle caselle di posta in arrivo di visualizzare il logo di un marchio accanto ai messaggi e-mail autenticati del marchio all'interno dei client e-mail di supporto.

BIMI è una specifica e-mail direttamente collegata all'autenticazione, ma non è un protocollo di autenticazione e-mail autonomo in quanto richiede che tutte le e-mail siano conformi all'autenticazione DMARC.

Sebbene BIMI richieda DMARC, DMARC richiede che il dominio disponga di record SPF o DKIM da allineare, ma è opportuno includere entrambi i record SPF e DKIM per una maggiore sicurezza e perché alcuni fornitori di servizi e-mail (ESP) richiedono entrambi quando si utilizza BIMI. Nella sezione seguente vengono illustrati i passaggi per implementare BIMI in Amazon SES.

Configurazione di BIMI in SES

Puoi configurare BIMI per un dominio e-mail di tua proprietà, in SES, che è noto come dominio MAIL FROM personalizzato. Dopo che è stato configurato, tutti i messaggi inviati da tale dominio visualizzeranno il logo BIMI nei client e-mail che supportano BIMI.

Per consentire alle e-mail di visualizzare un logo BIMI è necessario che SES contenga alcuni prerequisiti: nella procedura seguente, questi prerequisiti vengono generalizzati e fanno riferimento a sezioni dedicate che trattano questi argomenti in dettaglio. I passaggi specifici di BIMI e la relativa configurazione in SES saranno descritti in dettaglio qui.

Per configurare BIMI su un dominio MAIL FROM personalizzato

1. È necessario disporre di un dominio MAIL FROM personalizzato configurato in SES con record SPF (tipo TXT) e MX pubblicati per tale dominio. Se non disponi di un dominio MAIL FROM personalizzato o desideri crearne uno nuovo per il tuo logo BIMI, consultare the section called “Uso di un dominio MAIL FROM personalizzato”.
2. Configura il tuo dominio con Easy DKIM. Per informazioni, consultare the section called “Easy DKIM”.
3. Configura il tuo dominio con DMARC pubblicando un record TXT con il provider DNS con le seguenti specifiche della policy di applicazione richieste per BIMI:

Nome	Type (Tipo)	Value (Valore)
`_dmarc.example.com`	`TXT`	`v=DMARC1;p=quarantine;pct=100;rua=mailto:dmarcreports@example.com`
		`v=DMARC1;p=reject;rua=mailto:dmarcreports@example.com`

Nell'esempio di policy DMARC precedente come richiesto per BIMI:

- *`example.com`* deve essere sostituito con il nome di dominio o sottodominio.
- Il valore p= può essere:
  - quarantine con un valore pct impostato su 100 come mostrato, oppure
  - reject come mostrato.
- Se stai eseguendo l'invio da un sottodominio, BIMI richiede che anche il dominio padre disponga di questa policy di applicazione. I sottodomini ricadono nella policy del dominio padre. Tuttavia, se aggiungi un record DMARC per il sottodominio oltre a quello pubblicato per il dominio padre, anche il sottodominio deve avere la stessa policy di applicazione affinché sia idoneo per BIMI.
- Se non hai mai impostato una policy DMARC per il dominio, consulta the section called "Autenticazione delle e-mail con DMARC" per assicurati di utilizzare solo i valori della policy DMARC specifici per BIMI, come mostrato.

4. Produci il tuo logo BIMI come un file `.svg` SVG (Scalable Vector Graphics): il profilo SVG specifico richiesto da BIMI è definito come SVG Portable/Secure (SVG P/S). Affinché possa essere visualizzato nel client e-mail, il logo deve essere esattamente conforme a queste specifiche. Consultare le istruzioni di BIMI Group sulla creazione di file di logo SVG e gli strumenti di conversione SVG consigliati.
5. (Facoltativo) Ottieni un Verified Mark Certificate (VMC). Alcuni ESP, come Gmail e Apple, richiedono un VMC per fornire la prova che il marchio e il contenuto del logo BIMI sono di proprietà dell'utente. Sebbene questo non sia un requisito per implementare BIMI sul dominio, il logo BIMI non verrà visualizzato nel client e-mail se l'ESP a cui si invia la posta impone la conformità VMC. Consultare i riferimenti del BIMI Group alle autorità di certificazione dei partecipanti per ottenere un VMC per il logo.

6. Ospitare il file SVG del logo BIMI su un server a cui si ha accesso rendendolo accessibile pubblicamente tramite HTTPS. Ad esempio, è possibile caricarlo su un bucket Amazon S3.
7. Crea e pubblica un record DNS BIMI che include un URL al tuo logo. Quando un ESP che supporta BIMI controlla il record DMARC, cercherà anche un record BIMI contenente l'URL per il file `.svg` del logo e, se configurato, l'URL per il file `.pem` del VMC. Se i record corrispondono, il logo BIMI verrà visualizzato.

   Configura il dominio con BIMI pubblicando un record TXT con il provider DNS con i seguenti valori, come mostrato: l'invio da un dominio è rappresentato nel primo esempio; l'invio da un sottodominio è rappresentato nel secondo esempio:

Nome	Type (Tipo)	Value (Valore)
`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`		

   Negli esempi di record BIMI precedenti:

   - Il valore del nome deve specificare letteralmente `default._bimi.` come un sottodominio di *`example.com`* o *`marketing.example.com`* che deve essere sostituito con il nome del dominio o del sottodominio.
   - Il valore `v=` è la versione del record BIMI.
   - Il valore `l=` è il logo che rappresenta l'URL che punta al file `.svg` dell'immagine.
   - Il valore `a=` è l'autorità che rappresenta l'URL che punta al file `.pem` del certificato.

   Puoi convalidare il record BIMI con uno strumento come il BIMI Inspector del BIMI Group.

Il passaggio finale di questo processo consiste nell'avere uno modello di invio regolare agli ESP che supportano il posizionamento del logo BIMI. Il dominio deve avere una cadenza di consegna regolare e avere una buona reputazione presso gli ESP destinatari. Il posizionamento del logo BIMI può richiedere tempo per la compilazione negli ESP presso cui non si dispone di una reputazione o una cadenza di invio consolidate.

Ulteriori informazioni e risorse relative a BIMI sono disponibili tramite l'organizzazione BIMI Group.

Impostazione delle notifiche degli eventi per Amazon SES

Per inviare e-mail utilizzando Amazon SES, devi disporre di un sistema per la gestione di mancati recapiti e reclami. Amazon SES può effettuare la notifica degli eventi di mancata recapito o reclamo in tre modi: inviando una notifica e-mail, notificando un argomento Amazon SNS o pubblicando eventi di invio. Questa sezione contiene informazioni sulla configurazione di Amazon SES per l'invio di alcuni tipi di notifiche via e-mail o mediante notifica di un argomento Amazon SNS. Per ulteriori informazioni sulla pubblicazione di eventi, consulta l'argomento Monitoraggio dell'invio di e-mail utilizzando la pubblicazione di eventi di Amazon SES.

Puoi impostare le notifiche tramite la console Amazon SES o l'API Amazon SES.

Argomenti

Considerazioni importanti

Vi sono diversi punti importanti da considerare quando configuri Amazon SES per l'invio di notifiche:

- Le e-mail e le notifiche Amazon SNS si applicano alle identità individuali, ossia gli indirizzi e-mail o i domini verificati che utilizzi per inviare e-mail. Quando abiliti le notifiche per un'identità, Amazon SES invia notifiche solo per le e-mail inviate da tale identità e solo nella Regione AWS in cui hai configurato tali notifiche.
- Devi abilitare un metodo per la ricezione delle notifiche di mancato recapito e reclamo. Puoi inviare notifiche per il dominio o l'indirizzo e-mail che ha generato il mancato recapito o il reclamo a un argomento Amazon SNS. Puoi anche utilizzare la pubblicazione di eventi per inviare notifiche su diversi tipi di eventi (inclusi rimbalzi, reclami, consegne e altro) a un argomento Amazon SNS o a uno stream Firehose.

  Se non configuri uno di questi metodi per la ricezione delle notifiche di mancato recapito e reclamo, Amazon SES inoltra automaticamente le notifiche di mancato recapito e reclamo all'indirizzo del percorso di ritorno (o indirizzo di origine, se non hai specificato un percorso di ritorno) delle e-mail che hanno generato l'evento di mancato recapito o reclamo, anche nel caso in cui fosse disabilitato l'inoltro di feedback e-mail.

Se disabiliti l'inoltro di feedback e-mail e abiliti la pubblicazione di eventi, devi applicare il set di configurazione che contiene la regola di pubblicazione dell'evento a tutte le e-mail inviate. In questo caso, se non utilizzi il set di configurazione, Amazon SES inoltra automaticamente le notifiche di mancato recapito e reclamo all'indirizzo del percorso di ritorno o di origine delle e-mail che hanno generato l'evento di mancato recapito o reclamo.

- Se configuri Amazon SES per l'invio degli eventi di mancato recapito e reclamo usando più di un metodo (ad esempio inviando notifiche via e-mail e utilizzando la pubblicazione di eventi), potresti ricevere più di una notifica per lo stesso evento.

Ricezione delle notifiche Amazon SES tramite e-mail

Amazon SES può inviarti e-mail in caso di mancati recapiti e reclami utilizzando un processo denominato inoltro di feedback via e-mail.

Per inviare e-mail usando Amazon SES, devi configurarlo per l'invio delle notifiche di mancato recapito e reclamo utilizzando uno dei seguenti metodi:

- abilitando l'inoltro di feedback via e-mail; La procedura per la configurazione di questo tipo di notifica è incluso in questa sezione;
- inviando notifiche a un argomento Amazon SNS. Per ulteriori informazioni, consulta Ricezione di notifiche Amazon SES di Amazon utilizzando Amazon SNS.
- pubblicando le notifiche dell'evento. Per ulteriori informazioni, consulta Monitoraggio dell'invio di e-mail utilizzando la pubblicazione di eventi di Amazon SES.

> **Important**
>
> Per diversi punti importanti sulle notifiche, consulta Impostazione delle notifiche degli eventi per Amazon SES.

Argomenti

abilitando l'inoltro di feedback via e-mail;

L'inoltro di feedback via e-mail è abilitato per impostazione predefinita. Se in precedenza lo hai disabilitato, puoi abilitarlo seguendo le procedure in questa sezione.

Abilitazione dell'inoltro di mancati recapiti e reclami tramite e-mail utilizzando la console Amazon SES

1. Accedi alla AWS Management Console e apri la console Amazon SES all'indirizzo https://console.aws.amazon.com/ses/.
2. Nel pannello di navigazione, in Configuration (Configurazione), scegli Verified identities (Identità verificate).
3. Nell'elenco degli indirizzi e-mail e domini verificati, scegli l'indirizzo e-mail o il dominio per il quale desideri configurare le notifiche di mancato recapito e reclamo.
4. Nel pannello dei dettagli espandi la sezione Notifications (Notifiche).
5. Scegli Edit Configuration (Modifica configurazione).
6. In Email Feedback Forwarding (Inoltro feedback via e-mail), scegli Enabled (Abilitato).

> **Note**
>
> Potrebbero trascorrere alcuni minuti affinché le modifiche apportate alle impostazioni in questa pagina diventino effettive.

Puoi anche abilitare le notifiche di rimbalzi e reclami tramite e-mail utilizzando l'operazione SetIdentityFeedbackForwardingEnabledAPI.

Disabilitazione dell'inoltro di feedback via e-mail

Se configuri un metodo diverso per ottenere notifiche di mancato recapito e reclamo, puoi disattivare l'inoltro di feedback via e-mail, in modo da non ricevere più notifiche quando si verifica un evento di mancato recapito o reclamo.

Disabilitazione dell'inoltro di mancati recapiti e reclami tramite e-mail utilizzando la console Amazon SES

1. Accedi alla AWS Management Console e apri la console Amazon SES all'indirizzo https://console.aws.amazon.com/ses/.

2. Nel pannello di navigazione, in Configuration (Configurazione), scegli Verified identities (Identità verificate).
3. Nell'elenco degli indirizzi e-mail e domini verificati, scegli l'indirizzo e-mail o il dominio per il quale desideri configurare le notifiche di mancato recapito e reclamo.
4. Nel pannello dei dettagli espandi la sezione Notifications (Notifiche).
5. Scegli Edit Configuration (Modifica configurazione).
6. In Email Feedback Forwarding (Inoltro feedback via e-mail), scegli Disabled (Disabilitato).

> **Note**
>
> Devi configurare un metodo di ricezione delle notifiche di mancato recapito e reclamo per inviare e-mail tramite Amazon SES. Se disabiliti l'inoltro del feedback via e-mail, devi abilitare le notifiche inviate da Amazon SNS o pubblicare eventi di rimbalzo e reclamo su un argomento di Amazon SNS o uno stream Firehose utilizzando la pubblicazione di eventi. Se usi la pubblicazione di eventi, devi inoltre applicare il set di configurazione che contiene la regola di pubblicazione dell'evento per ogni e-mail inviata. Se non configuri un metodo per la ricezione delle notifiche di mancato recapito e reclamo, Amazon SES inoltra automaticamente le notifiche di mancato recapito e reclamo all'indirizzo indicato nel campo del percorso di ritorno (o nel campo dell'indirizzo di origine, se non hai specificato un percorso di ritorno) del messaggio che ha generato l'evento di mancato recapito o reclamo. In questo caso, Amazon SES inoltra notifiche di mancato recapito e reclamo anche se hai disabilitato le notifiche di feedback.

7. Scegli Save Config (Salva configurazione) per salvare la tua configurazione delle notifiche.

> **Note**
>
> Potrebbero volerci alcuni minuti affinché le modifiche apportate alle impostazioni in questa pagina diventino effettive.

Puoi anche disabilitare le notifiche di rimbalzi e reclami tramite e-mail utilizzando l'operazione API. SetIdentityFeedbackForwardingEnabled

Destinazione dell'inoltro di feedback via e-mail

Quando ricevi una notifica tramite e-mail, Amazon SES riscrive l'intestazione `From` e ti invia la notifica. L'indirizzo a cui Amazon SES inoltra la notifica dipende dal modo in cui hai inviato il messaggio originale.

Se per inviare il messaggio hai utilizzato l'interfaccia SMTP, le notifiche vengono consegnate in base alle seguenti regole:

- Se hai specificato un'intestazione `Return-Path` nella sezione `SMTP DATA`, allora le notifiche arrivano a quell'indirizzo.
- In caso contrario, le notifiche vengono inviate all'indirizzo specificato quando è stato emesso il comando MAIL FROM.

Se per inviare il messaggio hai utilizzato l'operazione API `SendEmail`, le notifiche vengono consegnate in base alle seguenti regole:

- Se hai specificato il parametro opzionale `ReturnPath` nella chiamata all'API `SendEmail`, le notifiche arrivano a quell'indirizzo.
- In caso contrario, le notifiche arrivano all'indirizzo specificato nel parametro obbligatorio `Source` di `SendEmail`.

Se per inviare il messaggio hai utilizzato l'operazione API `SendRawEmail`, le notifiche vengono consegnate in base alle seguenti regole:

- Se hai specificato un'intestazione `Return-Path` nel messaggio RAW, le notifiche arrivano a quell'indirizzo.
- Se hai specificato il parametro `Source` nella chiamata all'API `SendRawEmail`, le notifiche arrivano a quell'indirizzo.
- In caso contrario, le notifiche arrivano all'indirizzo specificato nell'intestazione `From` del messaggio in formato RAW.

> **Note**
>
> Quando specifichi un indirizzo `Return-Path` in un'e-mail, ricevi le notifiche a quell'indirizzo. Tuttavia, la versione del messaggio ricevuto dal destinatario contiene un'intestazione `Return-Path` che include un indirizzo e-mail anonimo (ad esempio a0b1c2d3e4f5a6b7-

c8d9e0f1-a2b3-c4d5-e6f7-a8b9c0d1e2f3-000000@amazonses.com). Questa perdita di identità avviene indipendentemente dal modo in cui è stata inviata l'e-mail.

Ricezione di notifiche Amazon SES di Amazon utilizzando Amazon SNS

Puoi configurare Amazon SES per notificare un argomento Amazon SNS quando ricevi messaggi non recapitati o reclami oppure quando le e-mail vengono consegnate. Le notifiche di Amazon SNS sono in formato JavaScript Object Notation (JSON), che ne permette l'elaborazione a livello di programmazione.

Per inviare e-mail usando Amazon SES, devi configurarlo per l'invio delle notifiche di mancato recapito e reclamo utilizzando uno dei seguenti metodi:

- inviando notifiche a un argomento Amazon SNS. La procedura per la configurazione di questo tipo di notifica è incluso in questa sezione;
- abilitando l'inoltro di feedback via e-mail; Per ulteriori informazioni, consulta Ricezione delle notifiche Amazon SES tramite e-mail.
- pubblicando le notifiche dell'evento. Per ulteriori informazioni, consulta Monitoraggio dell'invio di e-mail utilizzando la pubblicazione di eventi di Amazon SES.

> **Important**
>
> Per informazioni importanti sulle notifiche, consulta Impostazione delle notifiche degli eventi per Amazon SES.

Argomenti

- Configurazione delle notifiche Amazon SNS per Amazon SES
- Contenuti delle notifiche Amazon SNS per Amazon SES
- Esempi delle notifiche Amazon SNS per Amazon SES

Configurazione delle notifiche Amazon SNS per Amazon SES

Amazon SES può notificarti i tuoi mancati recapiti, i tuoi reclami e i messaggi recapitati tramite Amazon Simple Notification Service (Amazon SNS).

È possibile configurare le notifiche nella console Amazon SES oppure usando l'API Amazon SES.

Argomenti in questa sezione:

Prerequisiti

Completa le fasi seguenti prima di configurare le notifiche Amazon SNS in Amazon SES:

1. Crea un argomento in Amazon SNS. Per ulteriori informazioni, consulta la pagina Creazione di un argomento nella Guida per gli sviluppatori di Amazon Simple Notification Service.

   > **Important**
   >
   > Quando crei il tuo argomento utilizzando Amazon SNS, per Type (Tipo), scegli solo Standard. (SES non supporta argomenti di tipo FIFO).

   Sia che crei un nuovo argomento SNS o ne selezioni uno esistente, è necessario concedere l'accesso a SES per pubblicare le notifiche sull'argomento.

   Per concedere ad Amazon SES l'autorizzazione a pubblicare notifiche nell'argomento, nella schermata Edit topic (Modifica argomento) della console SNS, espandi Access policy (Policy di accesso) e in JSON editor (Editor JSON), aggiungi la policy di autorizzazione che segue:

```
{
  "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"
        }
      }
    }
  ]
}
```

Nel precedente esempio di policy, apporta le modifiche seguenti:

- Sostituisci *topic_region* con la regione AWS in cui hai creato l'argomento SNS.
- Sostituisci *111122223333* con l'ID del tuo account AWS.
- Sostituisci *topic_name* con il nome del tuo argomento SNS.
- Sostituisci *identity_name* con l'identità verificata (indirizzo e-mail o dominio) a cui stai sottoscrivendo l'argomento SNS.

2. Effettua la sottoscrizione di almeno un endpoint per l'argomento. Se, ad esempio, desideri ricevere notifiche tramite messaggio di testo, effettua la sottoscrizione di un endpoint SMS, ovvero un numero di telefono cellulare, per l'argomento. Per ricevere le notifiche tramite e-mail, effettua la sottoscrizione di un endpoint e-mail (un indirizzo e-mail) per l'argomento.

   Per ulteriori informazioni, consulta Nozioni di base nella Guida per gli sviluppatori di Amazon Simple Notification Service.

3. (Opzionale) Se l'argomento Amazon SNS utilizza AWS Key Management Service (AWS KMS) per la crittografia lato server, devi aggiungere autorizzazioni alla policy delle chiavi AWS KMS. Puoi aggiungere autorizzazioni collegando la policy seguente alla policy delle chiavi AWS KMS:

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

```
                "kms:GenerateDataKey",
                "kms:Decrypt"
            ],
            "Resource": "*"
        }
    ]
}
```

Configurazione di notifiche tramite la console Amazon SES

Configurazione delle notifiche tramite la console Amazon SES

1. Aprire la console Amazon SES all'indirizzo https://console.aws.amazon.com/ses/.
2. Nel pannello di navigazione, in Configuration (Configurazione), scegli Verified identities (Identità verificate).
3. Nel container Identities (Identità), seleziona l'identità verificata per cui desideri ricevere notifiche di feedback in caso di mancato recapito, reclamo o consegna dei messaggi inviati.

> **Important**
>
> Le impostazioni di notifica dei domini verificati si applicano a tutte le e-mail inviate dagli indirizzi in tale dominio ad eccezione degli indirizzi e-mail che sono anch'essi verificati.

4. Nella schermata dei dettagli dell'identità verificata selezionata, scegli la scheda Notifications (Notifiche) e seleziona Edit (Modifica) nel container Feedback notifications (Notifiche di feedback).
5. Espandi la casella dell'elenco di argomenti SNS di ogni tipo di feedback per cui desideri ricevere notifiche e seleziona un argomento SNS di cui sei proprietario, No SNS topic (Nessun argomento SNS) o SNS topic you don't own (Argomento SNS che non possiedi).

    - Se scegli SNS topic you don't own (Argomento SNS che non possiedi), verrà visualizzato il campo SNS topic ARN (ARN dell'argomento SNS), in cui devi inserire l'ARN dell'argomento SNS condiviso con te dal mittente delegato. Solo il mittente delegato riceverà queste notifiche, perché è proprietario dell'argomento SNS. Per ulteriori informazioni sull'invio di delegati, consulta Panoramica dell'autorizzazione di invio.)

> **Important**
>
> Gli argomenti Amazon SNS utilizzati per le notifiche di mancato recapito, reclamo e consegna devono trovarsi nella stessa Regione AWS che utilizza Amazon SES. Inoltre, è necessario sottoscrivere uno o più endpoint all'argomento per ricevere le notifiche. Se, ad esempio, desideri ricevere le notifiche a un indirizzo e-mail, devi effettuare la sottoscrizione di un endpoint e-mail all'argomento. Per ulteriori informazioni, consulta Nozioni di base nella Guida per gli sviluppatori di Amazon Simple Notification Service.

6. (Facoltativo) Se desideri che la notifica dell'argomento includa le intestazioni dall'e-mail originale, seleziona la casella Include original email headers (Includi intestazioni e-mail originali) direttamente sotto il nome dell'argomento SNS di ogni tipo di feedback. Questa opzione è disponibile solo se hai assegnato un argomento Amazon SNS al tipo di notifica associato. Per informazioni sui contenuti delle intestazioni e-mail originali, consulta l'oggetto `mail` in Contenuti delle notifiche.
7. Scegliere Save changes (Salva modifiche). Potrebbero essere necessari alcuni minuti perché le modifiche apportate alle impostazioni di notifica diventino effettive.
8. (Facoltativo) Se scegli di abilitare le notifiche dell'argomento Amazon SNS sia per i mancati recapiti che per i reclami, puoi disabilitare completamente le notifiche e-mail in modo da non riceverle tramite entrambi i canali. Per disabilitare le notifiche e-mail per mancati recapiti e reclami, nella scheda Notifications (Notifiche) della schermata dei dettagli dell'identità verificata, vai al container Email Feedback Forwarding (Inoltro feedback e-mail), scegli Edit (Modifica), deseleziona la casella Enabled (Abilitato) e scegli Save changes (Salva modifiche).

Dopo aver configurato le impostazioni, inizierai a ricevere le notifiche di mancato recapito, reclamo e/o consegna per l'argomento o gli argomenti Amazon SNS. Queste notifiche sono in formato JSON (JavaScript Object Notation) e seguono la struttura descritta in Contenuti delle notifiche.

Per le notifiche di mancato recapito, reclamo e consegna ti verranno addebitate le tariffe standard di Amazon SNS. Per ulteriori informazioni, consulta la pagina dei prezzi di Amazon SNS.

> **Note**
>
> Se un tentativo di pubblicazione nell'argomento Amazon SNS non riesce perché l'argomento è stato eliminato o l'Account AWS non dispone più delle autorizzazioni per la pubblicazione,

Amazon SES rimuove la configurazione di tale argomento se è stato configurato per mancati recapiti o reclami (non le consegne: per le notifiche di consegna, SES non eliminerà l'impostazione di configurazione dell'argomento SNS). Inoltre, Amazon SES abilita nuovamente le notifiche e-mail di mancato recapito e reclamo per l'identità e riceverai una notifica della modifica tramite e-mail. Se sono configurate più identità per utilizzare l'argomento, la configurazione dell'argomento per ogni identità viene modificata quando in ogni identità si verifica un errore di pubblicazione nell'argomento.

Configurazione di notifiche tramite l'API Amazon SES

È anche possibile configurare le notifiche di mancato recapito, reclamo e consegna usando l'API Amazon SES. Per configurare le notifiche, usa le operazioni seguenti:

- SetIdentityNotificationTopic
- SetIdentityFeedbackForwardingEnabled
- GetIdentityNotificationAttributes
- SetIdentityHeadersInNotificationsEnabled

Puoi usare queste operazioni dell'API per scrivere un'applicazione front-end personalizzata per le notifiche. Per una descrizione completa delle operazioni dell'API correlate alla verifica del dominio, consulta la Documentazione di riferimento dell'API Amazon Simple Email Service.

Risoluzione dei problemi relativi alle notifiche di feedback

Nessuna notifica ricevuta

Se non ricevi notifiche, assicurati di aver sottoscritto un endpoint all'argomento a cui vengono inviate le notifiche. Quando effettui la sottoscrizione di un endpoint e-mail a un argomento, ricevi un'e-mail con la conferma di sottoscrizione. Devi confermare la sottoscrizione prima di iniziare a ricevere le notifiche e-mail. Per ulteriori informazioni, consulta Nozioni di base nella Guida per gli sviluppatori di Amazon Simple Notification Service.

Errore **`InvalidParameterValue`** durante la scelta di un argomento

Se ricevi un errore che indica `InvalidParameterValue`, controlla l'argomento Amazon SNS per vedere se è crittografato utilizzando AWS KMS. In caso affermativo, devi modificare la policy per la chiave AWS KMS. Consulta Prerequisiti per una policy di esempio.

Contenuti delle notifiche Amazon SNS per Amazon SES

Le notifiche di mancato recapito, reclamo e consegna vengono pubblicate in argomenti Amazon Simple Notification Service (Amazon SNS) in formato JavaScript Object Notation (JSON). L'oggetto JSON di primo livello contiene una stringa `notificationType`, un oggetto `mail` e un oggetto `bounce`, `complaint` o `delivery`.

Consulta le seguenti sezioni per la descrizione dei diversi tipi di oggetti:

- Oggetto JSON di primo livello
- Oggetto `mail`
- Oggetto `bounce`
- Oggetto `complaint`
- Oggetto `delivery`

Di seguito sono elencate alcune note importanti sui contenuti delle notifiche Amazon SNS per Amazon SES:

- Per un determinato tipo di notifica, puoi ricevere una notifica Amazon SNS per più destinatari oppure una singola notifica Amazon SNS per ogni destinatario. Il tuo codice deve essere in grado di analizzare la notifica Amazon SNS e gestire entrambi i casi. Amazon SES non garantisce l'ordine o il raggruppamento in batch delle notifiche inviate tramite Amazon SNS. Tuttavia, diversi tipi di notifica Amazon SNS (ad esempio, messaggi non recapitati e reclami) non saranno mai combinati in un'unica notifica.
- Puoi ricevere più tipi di notifica Amazon SNS per un destinatario. Ad esempio, il server di posta ricevente potrebbe accettare l'e-mail (attivando una notifica di consegna), ma dopo l'elaborazione dell'e-mail potrebbe determinare che si tratta in realtà di un mancato recapito e attivare una notifica di mancato recapito. Tuttavia, queste saranno sempre notifiche separate perché si tratta di diversi tipi di notifica.
- Amazon SES si riserva il diritto di aggiungere ulteriori campi alle notifiche. Per questo motivo, le applicazioni che analizzano tali notifiche devono essere sufficientemente flessibili per gestire campi sconosciuti.
- Amazon SES sovrascrive le intestazioni del messaggio quando invia l'e-mail. Puoi recuperare le intestazioni del messaggio originale dai campi `headers` e `commonHeaders` dell'oggetto `mail`.

Oggetto JSON di primo livello

L'oggetto JSON di primo livello in una notifica Amazon SES contiene i campi riportati di seguito.

Nome campo	Descrizione
`notificationType`	Una stringa che contiene il tipo di notifica rappresentato dall'oggetto JSON. I valori possibili sono `Bounce`, `Complaint` o `Delivery`. Se configuri la pubblicazione di eventi, questo campo è denominato `eventType`.
`mail`	Un oggetto JSON che contiene informazioni sull'e-mail originale a cui la notifica è correlata. Per ulteriori informazioni, consulta Oggetto mail.
`bounce`	Questo campo è presente solo se `notificationType` è `Bounce` e contiene un oggetto JSON che contiene informazioni sul mancato recapito. Per ulteriori informazioni, consulta Oggetto del mancato recapito.
`complaint`	Questo campo è presente solo se `notificationType` è `Complaint` e contiene un oggetto JSON che contiene informazioni sul reclamo. Per ulteriori informazioni, consulta Oggetto del reclamo.
`delivery`	Questo campo è presente solo se `notificationType` è `Delivery` e contiene un oggetto JSON che contiene informazioni sulla consegna. Per ulteriori informazioni, consulta Oggetto di consegna.

Oggetto mail

Ogni notifica di mancato recapito, reclamo o consegna contiene informazioni sull'e-mail originale nell'oggetto `mail`. L'oggetto JSON che contiene informazioni su un oggetto `mail` include i campi riportati di seguito.

Nome campo	Descrizione
`timestamp`	La data e l'ora in cui il messaggio originale è stato inviato (in formato ISO8601).
`messageId`	Un ID univoco che Amazon SES ha assegnato al messaggio. Amazon SES ti ha restituito questo valore quando hai inviato il messaggio. **Note** Questo è l'ID messaggio assegnato da Amazon SES. Puoi trovare l'ID messaggio dell'e-mail originale nei campi `headers` dell'oggetto `mail`.
`source`	L'indirizzo e-mail da cui il messaggio originale è stato inviato (indirizzo MAIL FROM della busta).
`sourceArn`	L'Amazon Resource Name (ARN) dell'identità utilizzata per inviare l'e-mail. Nel caso di autorizzazione all'invio, `sourceArn` è l'ARN dell'identità che il mittente delegato è stato autorizzato a utilizzare dal proprietario dell'identità per inviare l'e-mail. Per ulteriori informazioni sull'autorizzazione all'invio, consulta Metodi di autenticazione delle e-mail.
`sourceIp`	L'indirizzo IP pubblico di origine del client che ha eseguito la richiesta di invio di e-mail ad Amazon SES.

Nome campo	Descrizione
`sendingAccountId`	L'ID dell'account Account AWS utilizzato per inviare l'e-mail. Nel caso di autorizzazione all'invio, `sendingAccountId` è l'ID account del mittente delegato.
`callerIdentity`	L'identità IAM dell'utente di Amazon SES che ha inviato l'e-mail.
`destination`	Un elenco degli indirizzi e-mail destinatari della posta originale.
`headersTruncated`	Questo oggetto è presente solo se hai configurato le impostazioni di notifica affinché le stesse includano le intestazioni dall'e-mail originale. Indica se le intestazioni vengono troncate nella notifica. Amazon SES tronca le intestazi oni nella notifica quando le intestazioni dal messaggio originale hanno una dimensione pari a 10 KB o superiore. I valori possibili sono `true` e `false`.

Nome campo	Descrizione
`headers`	Questo oggetto è presente solo se hai configurato le impostazioni di notifica affinché le stesse includano le intestazioni dall'e-mail originale. Un elenco delle intestazioni originali dell'e-mail. Ogni intestazione nell'elenco include un campo `name` e un campo `value`. **Note** L'ID messaggio nell'oggetto `headers` deriva dal messaggio originale passato ad Amazon SES. L'ID messaggio che Amazon SES ha successivamente assegnato al messaggio si trova nel campo `messageId` dell'oggetto `mail`.

Nome campo	Descrizione
`commonHeaders`	Questo oggetto è presente solo se hai configurato le impostazioni di notifica affinché le stesse includano le intestazioni dall'e-mail originale. Include informazioni sulle intestazioni delle e-mail più comuni provenienti dall'e-mail originale , compresi i campi Da, A e Oggetto. Nell'ambito di questo oggetto, ogni intestazione rappresenta una chiave. I campi Da e A sono rappresentati da array che possono contenere più valori. **Note** Per gli eventi, qualsiasi ID messaggio all'interno del campo `commonHeaders` è quello che Amazon SES ha successivamente assegnato al messaggio nel campo `messageId` dell'oggetto mail. Le notifiche conterranno l'ID del messaggio dell'e-mail originale.

Di seguito è riportato un esempio di un oggetto `mail` che include le intestazioni dell'e-mail originale. Quando questo tipo di notifica non è configurato per includere le intestazioni dell'e-mail originale, l'oggetto `mail` non include i campi `headersTruncated`, `headers` e `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"
   }
```

```
}
```

Oggetto del mancato recapito

L'oggetto JSON che contiene informazioni sui mancati recapiti dispone dei campi riportati di seguito.

Nome campo	Descrizione
`bounceType`	Il tipo di mancato recapito secondo Amazon SES. Per ulteriori informazioni, consulta Tipi di mancato recapito.
`bounceSubType`	Il sottotipo di mancato recapito secondo Amazon SES. Per ulteriori informazioni, consulta Tipi di mancato recapito.
`bouncedRecipients`	Elenco che contiene informazioni sui destinatari della posta originale che non è stata recapitata. Per ulteriori informazioni, consulta Destinatari del mancato recapito.
`timestamp`	La data e l'ora in cui la notifica di mancato recapito è stata inviata (in formato ISO8601). Nota che questo è il momento in cui la notifica è stata inviata dall'ISP e non il momento in cui è stata ricevuta da Amazon SES.
`feedbackId`	Un ID univoco per il mancato recapito.

Se Amazon SES ha potuto contattare la Message Transfer Authority (MTA) remota, sarà presente anche il campo seguente.

Nome campo	Descrizione
`remoteMtaIp`	L'indirizzo IP dell'autorità MTA a cui Amazon SES ha tentato di consegnare l'e-mail.

Se una notifica sullo stato di consegna è stato associata al mancato recapito, sarà presente anche il campo seguente.

Nome campo	Descrizione
`reportingMTA`	Il valore del campo `Reporting-MTA` nella notifica sullo stato del recapito. Questo è il valore dell'autorità MTA che ha tentato di eseguire l'operazione di consegna, inoltro o gateway descritta nella notifica.

Di seguito è illustrato un esempio di oggetto `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"
}
```

Destinatari del mancato recapito

Una notifica di mancato recapito può riguardare uno o più destinatari. Il campo `bouncedRecipients` contiene un elenco di oggetti, uno per ogni destinatario interessato dalla notifica di mancato recapito e conterrà sempre il campo seguente.

Nome campo	Descrizione
`emailAddress`	L'indirizzo e-mail del destinatario. Se è disponibile una notifica sullo stato di consegna, questo è il valore del campo `Final-Recipient` della notifica.

Opzionalmente, se una notifica sullo stato di consegna è allegata al mancato recapito, possono essere presenti anche i campi seguenti.

Nome campo	Descrizione
`action`	Il valore del campo `Action` nella notifica sullo stato del recapito. Indica l'operazione eseguita dall'autorità MTA interessata come risultato del tentativo di recapitare il messaggio a questo destinatario.
`status`	Il valore del campo `Status` nella notifica sullo stato del recapito. Questo è il codice di stato indipendente dal trasporto che indica lo stato di consegna del messaggio per ogni destinatario.
`diagnosticCode`	Il codice di stato emesso dall'autorità MTA interessata. Si tratta del valore del campo `Diagnostic-Code` nella notifica sullo stato di consegna. Il campo potrebbe non essere incluso in questa notifica, quindi nemmeno nell'oggetto JSON.

Di seguito è riportato l'esempio di un oggetto che potrebbe essere incluso nell'elenco `bouncedRecipients`.

```
{
    "emailAddress": "recipient@example.com",
    "action": "failed",
```

```
    "status": "5.0.0",
    "diagnosticCode": "X-Postfix; unknown user"
}
```

Tipi di mancato recapito

L'oggetto di mancato recapito contiene un mancato recapito di tipo `Undetermined`, `Permanent` o `Transient`. Il mancato recapito di tipo `Transient` e `Permanent` possono anche contenere uno dei diversi sottotipi di mancato recapito.

Quando ricevi una notifica di mancato recapito di tipo `Transient`, potresti essere in grado di inviare e-mail a tale destinatario in futuro se il problema che ha causato il mancato recapito del messaggio viene risolto.

Quando ricevi una notifica di mancato recapito di tipo `Permanent`, difficilmente potrai inviare e-mail a tale destinatario in futuro. Per questo motivo, è consigliabile rimuovere immediatamente dalla tua mailing list il destinatario il cui indirizzo ha determinato il mancato recapito.

> **Note**
>
> Quando si verifica un soft bounce (e-mail non recapitata) (ossia un mancato recapito correlato a un problema temporaneo, ad esempio la casella di posta in arrivo dei destinatari è piena), Amazon SES tenta di consegnare nuovamente il messaggio e-mail per un determinato periodo di tempo. Al termine di tale periodo di tempo, se Amazon SES ancora non è in grado di consegnare l'e-mail, interrompe il tentativo.
> Amazon SES fornisce notifiche relative a hard bounce (mancato recapito permanente), nonché soft bounce (e-mail non recapitata) per i quali interrompe il tentativo di consegna. Se desideri ricevere una notifica ogni volta che si verifica un soft bounce (e-mail non recapitata), abilita la pubblicazione degli eventi e configurala per inviare notifiche quando si verificano eventi di ritardo nella consegna.

bounceType	bounceSubType	Descrizione
`Undetermined`	`Undetermined`	Il provider e-mail del destinatario ha inviato un messaggio di mancato recapito. Il messaggio di mancato recapito non contiene informazioni sufficienti affinché Amazon SES possa

bounceType	bounceSubType	Descrizione
		determinare il motivo di tale mancato recapito. L'e-mail di mancato recapito, inviata all'indirizzo Return-Path nell'intestazione dell'e-mail che ha generato il mancato recapito, potrebbe contenere ulteriori informazioni sul problema che ha determinato il mancato recapito dell'e-mail.
`Permanent`	`General`	Il provider e-mail del destinatario ha inviato un messaggio di mancato recapito permanente. **Important** Se ricevi questo tipo di notifica di mancato recapito (bounce), devi eliminare immediatamente l'indirizzo e-mail del destinatario dalla mailing list. L'invio di messaggi a indirizzi che producono un mancato recapito permanente può avere ripercussioni negative sulla tua reputazione come mittente. Se scegli di continuare a inviare e-mail a indirizzi che generano mancati recapiti permanenti, potremmo sospendere la tua capacità di inviare ulteriori e-mail. Per informazioni, consultare the section called “Utilizzo dell'elenco di eliminazione a livello di account”.
`Permanent`	`NoEmail`	Non è stato possibile recuperare l'indirizzo e-mail del destinatario dal messaggio di e-mail non recapitata.

bounceType	bounceSubType	Descrizione
`Permanent`	`Suppressed`	L'indirizzo e-mail del destinatario è sulla lista di eliminazione Amazon SES in quanto ha una storia recente di mancati recapiti permanent i. Per sovrascrivere l'elenco di eliminazione globale, consulta Utilizzo dell'elenco di eliminazi one a livello di account di Amazon SES.
`Permanent`	`OnAccountSuppressi onList`	Amazon SES ha soppresso l'invio a questo indirizzo perché si trova nell'elenco di eliminazi one a livello di account. Ciò non influisce sulla metrica relativa alla frequenza dei mancati recapiti.
`Transient`	`General`	Il provider di posta elettronica del destinatario ha inviato un messaggio generico di mancato recapito. Potresti essere in grado di inviare un messaggio allo stesso destinatario in futuro se il problema che ha determinato il messaggio di mancato recapito viene risolto. **Note** Se invii un'e-mail a un destinatario che ha una regola di risposta automatic a attiva (ad esempio un messaggio di "fuori sede"), potresti ricevere questo tipo di notifica. Anche se la risposta è un tipo di notifica `Bounce`, Amazon SES non considera le risposte automatiche quando calcola il tasso di mancato recapito per il tuo account.

bounceType	bounceSubType	Descrizione
`Transient`	`MailboxFull`	Il provider di posta elettronica del destinatario ha inviato un messaggio di mancato recapito in quanto la cartella della posta in arrivo del destinatario è piena. Potrai inviare e-mail allo stesso destinatario in futuro quando la casella di posta non sarà più piena.
`Transient`	`MessageTooLarge`	Il provider di posta elettronica del destinatario ha inviato un messaggio di mancato recapito in quanto il messaggio inviato era troppo grande. Potrai inviare un messaggio al medesimo destinatario riducendo le dimensioni del messaggio.
`Transient`	`ContentRejected`	Il provider di posta elettronica del destinatario ha inviato un messaggio di mancato recapito in quanto il messaggio inviato presenta contenuti per i quali il provider non consente l'utilizz o. Potrai inviare un messaggio al medesimo destinatario modificando il contenuto del messaggio.
`Transient`	`AttachmentRejected`	Il provider di posta elettronica del destinatario ha inviato un messaggio di mancato recapito in quanto il messaggio conteneva un allegato inaccettabile. Ad esempio, alcuni provider di posta elettronica potrebbero non accettare messaggi con allegati contenenti un determina to tipo di file ovvero messaggi con allegati di dimensioni molto grandi. Potrai inviare un messaggio al medesimo destinatario rimuovend o o modificando il contenuto dell'allegato.

Oggetto del reclamo

L'oggetto JSON che contiene informazioni sui reclami dispone dei campi riportati di seguito.

Nome campo	Descrizione
`complainedRecipients`	Un elenco che contiene informazioni sui destinatari che potrebbero essere responsabili del reclamo. Per ulteriori informazioni, consulta Destinatari che hanno inviato il reclamo.
`timestamp`	La data e l'ora in cui l'ISP ha inviato la notifica di reclamo, in formato ISO 8601. La data e l'ora indicate in questo campo potrebbero essere differenti dalla data e ora in cui Amazon SES ha ricevuto la notifica.
`feedbackId`	ID univoco associato al reclamo.
`complaintSubType`	Il valore del campo `complaintSubType` può essere null o `OnAccountSuppressionList` . Se il valore è `OnAccountSuppressionList` , Amazon SES ha accettato il messaggio, ma non ha tentato di inviarlo perché presente nell'elenco di eliminazione a livello di account.

Inoltre, se un report di feedback è associato al reclamo, potrebbero essere presenti i campi seguenti.

Nome campo	Descrizione
`userAgent`	Il valore del campo `User-Agent` nel report di feedback. Indica il nome e la versione del sistema che ha generato il report.

Nome campo	Descrizione
`complaintFeedbackType`	Il valore del campo `Feedback-Type` nel report di feedback ricevuto dall'ISP. Contiene il tipo di feedback.
`arrivalDate`	Il valore del campo `Arrival-Date` o `Received-Date` nel report di feedback (in formato ISO8601). Il campo potrebbe non essere incluso nel report, quindi nemmeno nell'oggetto JSON.

Di seguito è illustrato un esempio di oggetto `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"
}
```

Destinatari che hanno inviato il reclamo

Il campo `complainedRecipients` contiene un elenco di destinatari che potrebbero aver inviato il reclamo. Ti consigliamo di utilizzare queste informazioni per determinare quale destinatario ha inviato il reclamo e quindi rimuovere immediatamente quel destinatario dalle tue liste mailing list.

> **Important**
>
> Molti ISP rimuovono l'indirizzo e-mail del destinatario che ha inviato il reclamo dalla loro notifica di reclamo. Per questo motivo, l'elenco contiene informazioni sui destinatari che potrebbe aver inviato il reclamo, in base ai destinatari del messaggio originale e all'ISP da cui

abbiamo ricevuto il reclamo. Amazon SES esegue una ricerca rispetto al messaggio originale per determinare l'elenco dei destinatari.

Gli oggetti JSON in questo elenco contengono il campo seguente.

Nome campo	Descrizione
`emailAddress`	L'indirizzo e-mail del destinatario.

Di seguito è illustrato un esempio di oggetto con reclamo del destinatario.

```
{ "emailAddress": "recipient1@example.com" }
```

> **Note**
>
> A causa di questo comportamento, puoi essere più certo di individuare l'indirizzo e-mail che ha inviato il reclamo sul tuo messaggio se limiti l'invio a un messaggio per ciascun destinatario (piuttosto che inviare un messaggio con 30 diversi indirizzi e-mail nella riga Ccn).

Tipi di reclamo

Puoi visualizzare i tipi di reclamo seguenti nel campo `complaintFeedbackType`, assegnati dall'ISP che effettua la segnalazione, secondo il sito Web IANA (Internet Assigned Numbers Authority):

- `abuse`: indica e-mail non richieste o altro tipo di e-mail illecite.
- `auth-failure`: report di errore di autenticazione dell'e-mail.
- `fraud`: indica una frode o attività di phishing.
- `not-spam`: indica che l'entità che fornisce il report non considera il messaggio come spam. Può essere utilizzato per correggere un messaggio che è stato erroneamente contrassegnato o classificato come spam.
- `other`: indica qualsiasi altro feedback che non rientra in altri tipi registrati.
- `virus`: segnala la presenza di un virus nel messaggio di origine.

Oggetto di consegna

L'oggetto JSON che contiene informazioni sulle consegne presenta sempre i campi riportati di seguito.

Nome campo	Descrizione
`timestamp`	La data e l'ora in cui Amazon SES ha consegnato l'e-mail al server di posta del destinatario (in formato ISO8601).
`processingTimeMillis`	Il tempo in millisecondi tra quando Amazon SES ha accettato la richiesta del mittente e il trasferimento del messaggio al server di posta del destinatario.
`recipients`	Un elenco dei destinatari dell'e-mail a cui si applica la notifica di consegna.
`smtpResponse`	Il messaggio di risposta SMTP dell'ISP remoto che ha accettato l'e-mail da Amazon SES. Questo messaggio può variare in base all'e-mai l, al server di posta ricevente e all'ISP ricevente .
`reportingMTA`	Il nome host del server di posta Amazon SES che ha inviato l'e-mail.
`remoteMtaIp`	L'indirizzo IP dell'autorità MTA a cui Amazon SES ha consegnato l'e-mail.

Di seguito è illustrato un esempio di oggetto `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"
}
```

Esempi delle notifiche Amazon SNS per Amazon SES

Le seguenti sezioni forniscono esempi dei tre tipi di notifiche:

- Per le notifiche di mancato recapito, consulta Esempi di notifiche di mancato recapito di Amazon SNS.
- Per le notifiche di reclamo, consulta Esempi di notifiche di reclamo di Amazon SNS.
- Per le notifiche di consegna, consulta Esempio di notifica di consegna Amazon SNS.

Esempi di notifiche di mancato recapito di Amazon SNS

Questa sezione contiene esempi di notifiche di mancato recapito con e senza una notifica sullo stato di consegna fornita dal ricevitore e-mail che ha inviato il feedback.

Notifica di mancato recapito con notifica sullo stato di consegna

Di seguito è riportato un esempio di notifica di mancato recapito contenente una notifica sullo stato di consegna e le intestazioni e-mail originali. Quando le notifiche di mancato recapito (bounce) non sono configurate per includere le intestazioni e-mail originali, l'oggetto `mail` nelle notifiche non include i campi `headersTruncated`, `headers` e `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"
          }
       }
   }
```

Notifica di mancato recapito senza notifica sullo stato di consegna

Di seguito è riportato un esempio di notifica di mancato recapito che include le intestazioni e-mail originali, ma non una notifica sullo stato di consegna. Quando le notifiche di mancato recapito (bounce) non sono configurate per includere le intestazioni e-mail originali, l'oggetto `mail` nelle notifiche non include i campi `headersTruncated`, `headers` e `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"
      }
   }
}
```

Esempi di notifiche di reclamo di Amazon SNS

Questa sezione contiene esempi di notifiche di reclamo con e senza un report di feedback fornito dal ricevitore e-mail che ha inviato il feedback.

Notifica di reclamo con report di feedback

Di seguito è riportato un esempio di notifica di reclamo contenente un report di feedback e le intestazioni e-mail originali. Quando le notifiche di reclamo non sono configurate per includere le intestazioni e-mail originali, l'oggetto `mail` nelle notifiche non include i campi `headersTruncated`, `headers` e `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"
       }
    }
  }
```

Notifica di reclamo senza report di feedback

Di seguito è riportato un esempio di notifica di reclamo che include le intestazioni e-mail originali, ma non un report di feedback. Quando le notifiche di reclamo non sono configurate per includere le intestazioni e-mail originali, l'oggetto `mail` nelle notifiche non include i campi `headersTruncated`, `headers` e `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"
         }
```

```
    }
}
```

Esempio di notifica di consegna Amazon SNS

Di seguito è riportato un esempio di notifica di consegna che include le intestazioni e-mail originali. Quando le notifiche di consegna non sono configurate per includere le intestazioni e-mail originali, l'oggetto `mail` nelle notifiche non include i campi `headersTruncated`, `headers` e `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 dell'autorizzazione dell'identità in Amazon SES

Le policy di autorizzazione dell'identità definiscono in che modo le singole identità verificate possono utilizzare Amazon SES specificando quali azioni dell'API SES sono consentite o negate per l'identità e in quali condizioni.

Mediante l'uso di queste policy di autorizzazione, puoi mantenere il controllo sulle tue identità, modificando o revocando le autorizzazioni in qualsiasi momento. Puoi anche autorizzare altri utenti a utilizzare identità di cui sei proprietario (domini o indirizzi e-mail) usando i loro account SES.

Argomenti

Anatomia della policy Amazon SES

Le policy aderiscono a una struttura specifica, contengono elementi e devono soddisfare determinati requisiti.

Struttura delle policy

Ogni policy di autorizzazione è un documento JSON collegato a un'identità. Ogni policy include le sezioni seguenti:

- informazioni specifiche della policy nella parte superiore del documento;
- una o più istruzioni singole, ciascuna delle quali descrive un set di autorizzazioni.

La policy di esempio seguente concede all'ID account AWS 123456789012 le autorizzazioni specificate nella sezione Azione per il dominio verificato 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"
      ]
    }
  ]
}
```

Puoi trovare ulteriori esempi di policy di autorizzazione in Esempi di policy di identità.

Elementi delle policy

Questa sezione descrive gli elementi contenuti nelle policy di autorizzazione dell'identità. Prima di tutto descriveremo gli elementi specifici della policy, quindi gli elementi che si applicano solo all'istruzione in cui sono inclusi. Seguirà una descrizione di come aggiungere condizioni alle istruzioni.

Per informazioni specifiche sulla sintassi degli elementi, consulta la sezione relativa alla grammatica del linguaggio delle policy IAM nella Guida per l'utente di IAM.

Informazioni specifiche della policy

Esistono due elementi specifici della policy: `Id` e `Version`. La tabella seguente fornisce informazioni su questi elementi.

Nome	Descrizione	Obbligatorio	Valori validi
`Id`	Identifica in modo univoco la policy.	No	Qualsiasi stringa
`Version`	Specifica la versione del linguaggio di accesso della policy.	No	Qualsiasi stringa. Come best practice consigliamo di includere questo campo con il valore "2012-10-17".

Istruzioni specifiche della policy

Le policy di autorizzazione dell'identità devono includere almeno un'istruzione. Ogni istruzione può includere gli elementi descritti nella tabella seguente.

Nome	Descrizione	Obbligatorio	Valori validi
`Sid`	Identifica in modo univoco l'istruzione.	No	Qualsiasi stringa.
`Effect`	Specifica il risultato che deve essere restituito dall'istr uzione della policy in fase di valutazione.	Sì	"Allow" o "Deny".
`Resource`	Specifica l'identità cui si applica la policy. Per autorizzazione di invio, si tratta del dominio o dell'indi rizzo e-mail che il proprietario di identità autorizza il mittente delegato a usare.	Sì	Il nome della risorsa Amazon (ARN) dell'identità.
`Principal`	Specifica l'utente Account AWS o il servizio AWS che riceve l'autorizzazione nell'istruzione.	Sì	Un ID Account AWS, ARN utente o servizio AWS valido. Account AWS Gli ID e gli ARN degli utenti vengono specificati utilizzando `"AWS"` (ad esempio, `"AWS": ["123456789012"]` o `"AWS": ["arn:aws:iam::123456789012:root"]`). I nomi del servizio AWS vengono

Nome	Descrizione	Obbligatorio	Valori validi
			specificati usando `"Service"` (ad esempio, `"Service": ["cognito-idp.amazonaws.com"]`). Per esempi di formato degli ARN utente, consulta Riferimenti generali di AWS.

Nome	Descrizione	Obbligatorio	Valori validi
`Action`	Specifica l'azione alla quale si applica l'istruzione.	Sì	"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",

Nome	Descrizione	Obbligatorio	Valori validi
			"ses:UntagResource", "ses:UpdateEmailIdentityPolicy" (Azioni di autorizzazione di invio: "ses:SendEmail", "ses:SendRawEmail", "ses:SendTemplatedEmail", "ses:SendBulkTemplatedEmail") Puoi specificare una o più di queste operazioni.
`Condition`	Specifica eventuali restrizioni o dettagli relativi all'autorizzazione.	No	Consulta le informazioni sulle condizioni che seguono questa tabella.

Condizioni

Una condizione è qualsiasi restrizione riguardo all'autorizzazione inclusa nell'istruzione. La parte dell'istruzione che specifica le condizioni può essere la più dettagliata di tutte le parti. Una chiave è la caratteristica specifica sui cui si basa la restrizione di accesso, ad esempio la data e l'ora della richiesta.

Usa insieme condizioni e chiavi per esprimere la limitazione. Ad esempio, se vuoi impedire al mittente delegato di inviare richieste ad Amazon SES per tuo conto dopo il 30 luglio 2019, devi usare la condizione denominata `DateLessThan`. Usi la chiave denominata `aws:CurrentTime` e la imposti sul valore `2019-07-30T00:00:00Z`.

Amazon SES implementa solo le seguenti chiavi di policy AWS:

- `aws:CurrentTime`
- `aws:EpochTime`

- `aws:SecureTransport`
- `aws:SourceIp`
- `aws:SourceVpc`
- `aws:SourceVpce`
- `aws:UserAgent`
- `aws:VpcSourceIp`

Per ulteriori informazioni su queste chiavi, consulta la Guida per l'utente IAM.

Requisiti per le policy

Le policy devono soddisfare tutti i seguenti requisiti:

- Ogni policy deve includere almeno un'istruzione.
- Ogni policy deve includere almeno un'entità principale valida.
- Ogni policy deve specificare una risorsa e tale risorsa deve essere l'ARN dell'identità a cui la policy è collegata.
- I proprietari di identità possono associare fino a 20 policy a ogni identità univoca.
- Le dimensioni delle policy non possono superare i 4 kilobyte (KB).
- I nomi delle policy non possono superare i 64 caratteri. Inoltre, possono includere solo caratteri alfanumerici, trattini e caratteri di sottolineatura.

Creazione di una policy di autorizzazione identità in Amazon SES

Una policy di autorizzazione identità comprende dichiarazioni che specificano quali azioni API sono consentite o negate per un'identità e in quali condizioni.

Per autorizzare un'identità dominio o indirizzo e-mail Amazon SES di tua proprietà, devi creare una policy di autorizzazione di invio e quindi collegare tale policy all'identità. Un'identità può avere zero, una o più policy. Tuttavia, una singola policy può essere associata solo a una singola identità.

Per un elenco delle azioni API che possono essere utilizzate in una policy di autorizzazione dell'identità, consulta la riga Azione nella tabella the section called “Istruzioni specifiche della policy”.

È possibile creare una policy di autorizzazione dell'identità nei modi seguenti:

- Usando il generatore di policy: puoi creare una policy semplice usando il generatore di policy nella console SES. Oltre a consentire o negare le autorizzazioni sulle azioni API SES, puoi vincolare le azioni con condizioni. Puoi anche usare il generatore di policy per creare rapidamente la struttura di base di una policy, quindi personalizzarla in un secondo momento modificando la policy.
- Creando una policy personalizzata: se desideri includere condizioni più avanzate o usare un servizio AWS; come principale, puoi creare una policy personalizzata e collegarla all'identità usando la console SES o l'API SES.

Argomenti

Uso del generatore di policy

Puoi usare il generatore di policy per creare una semplice policy di autorizzazione seguendo i passaggi indicati.

Creazione di una policy usando il generatore di policy

1. Accedere alla AWS Management Console e aprire la console Amazon SES all'indirizzo https://console.aws.amazon.com/ses/.
2. Nel pannello di navigazione, in Configuration (Configurazione), scegli Verified identities (Identità verificate).
3. Nel container Identities (Identità) della schermata Verified identities (Identità verificate), seleziona l'identità per la quale desideri creare una policy di autorizzazione.
4. Nella schermata dei dettagli dell'identità verificata selezionata nel passaggio precedente, scegli la scheda Authorization (Autorizzazione).
5. Nel riquadro Authorization policies (Policy di autorizzazione), scegli Create policy (Crea policy) e seleziona Use policy generator (Usa generatore di policy) dal menu a discesa.
6. Nel riquadro Create statement (Crea istruzione), scegli Allow (Consenti) nel campo Effect (Effetto). Se invece desideri creare una policy per limitare questa identità, scegli Deny (Nega).
7. Nel campo Principals (Principali), inserisci l'ID Account AWS, l'ARN utente IAM o il servizio AWS per ricevere le autorizzazioni che desideri autorizzare per questa identità, quindi scegli Add (Aggiungi). Se desideri autorizzarne più di una, ripeti questo passaggio per ciascuna.

8. Nel campo Actions (Azioni), seleziona la casella di controllo per ogni azione che desideri autorizzare per i principali.
9. (Facoltativo) Espandi Specify conditions (Specifica condizioni) se desideri aggiungere un'istruzione di qualificazione all'autorizzazione.
    a. Seleziona un operatore dal menu a discesa Operator (Operatore).
    b. Seleziona un tipo di chiave dal menu a discesa Key (Chiave).
    c. In base al tipo di chiave selezionato, inserisci il valore corrispondente nel campo Value (Valore). Se desideri aggiungere altre condizioni, scegli Add new condition (Aggiungi nuova condizione) e ripeti questo passaggio per ciascuna di esse.
10. Scegli Save statement (Salva istruzione).
11. (Facoltativo) Se desideri aggiungere altre istruzioni alla tua policy, espandi Create another statement (Crea un'altra istruzione) e ripeti i passaggi da 6 a 10.
12. Scegli Next (Successivo) e nella schermata Customize policy (Personalizza policy), il container Edit policy details (Modifica dettagli policy) dispone di campi in cui puoi modificare o personalizzare le voci Name (Nome) e Policy document (Documento policy).
13. Scegli Next (Successivo) e nella schermata Review and apply (Rivedi e applica), il container Overview (Panoramica) mostrerà l'identità verificata che stai autorizzando per il mittente delegato, nonché il nome di questa policy. Nel riquadro Policy document (Documento policy) sarà presente la policy effettiva che hai appena scritto insieme a tutte le condizioni che hai aggiunto: controlla la policy e, se sembra corretta, scegli Apply policy (Applica policy). Se hai bisogno di modificare o correggere qualcosa, scegli Previous (Precedente) e lavora nel container Edit policy details (Modifica dettagli policy).

Creazione di una policy personalizzata

Se desideri creare una policy personalizzata e collegarla a un'identità, hai a disposizione le seguenti opzioni:

- Uso dell'API Amazon SES: puoi creare una policy in un editor di testo, quindi collegarla all'identità usando l'API `PutIdentityPolicy` descritta nella Documentazione di riferimento per le API Amazon Simple Email Service.
- Uso della console Amazon SES: puoi creare una policy in un editor di testo e collegarla a un'identità incollandola nell'editor di policy personalizzate nella console Amazon SES. Questo metodo viene descritto nella procedura seguente.

Creazione di una policy personalizzata usando l'editor di policy personalizzate

1. Accedere alla AWS Management Console e aprire la console Amazon SES all'indirizzo https://console.aws.amazon.com/ses/.
2. Nel pannello di navigazione, in Configuration (Configurazione), scegli Verified identities (Identità verificate).
3. Nel container Identities (Identità) della schermata Verified identities (Identità verificate), seleziona l'identità per la quale desideri creare una policy di autorizzazione.
4. Nella schermata dei dettagli dell'identità verificata selezionata nel passaggio precedente, scegli la scheda Authorization (Autorizzazione).
5. Nel riquadro Authorization policies (Policy di autorizzazione), scegli Create policy (Crea policy) e seleziona Create custom policy (Crea policy personalizzata) dal menu a discesa.
6. Nel riquadro Policy document (Documento policy), digita o incolla il testo della policy nel formato JSON. Puoi anche usare il generatore di policy per creare rapidamente la struttura di base di una policy e personalizzarla qui.
7. Scegli Apply Policy (Applica policy). Se hai bisogno di modificare la policy personalizzata, seleziona la relativa casella di controllo sotto la scheda Authorization (Autorizzazione), scegli Edit (Modifica) e apporta le modifiche nel riquadro Policy document (Documento policy) seguito da Save changes (Salva modifiche).

Esempi di policy di identità in Amazon SES

L'autorizzazione dell'identità consente di specificare le condizioni dettagliate in base alle quali consentire o negare le azioni API per un'identità.

Gli esempi seguenti mostrano come scrivere policy per controllare diversi aspetti delle azioni API:

- Specifica del principale
- Limitazione dell'azione
- Uso di più istruzioni

Specifica del principale

Il principale, ossia l'entità cui concedi l'autorizzazione, può essere un Account AWS, un utente AWS Identity and Access Management (IAM) o un servizio AWS che appartiene allo stesso account.

L'esempio seguente mostra una semplice policy che permette all'ID AWS 123456789012 di controllare l'identità verificata example.com anch'essa di proprietà di Account 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 policy di esempio seguente concede a due utenti l'autorizzazione necessaria per controllare l'identità verificata example.com. Gli utenti vengono specificati tramite il rispettivo nome della risorsa 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"
      ]
    }
  ]
}
```

Limitazione dell'azione

Esistono diverse azioni che possono essere specificate in una policy di autorizzazione dell'identità a seconda del livello di controllo che si desidera autorizzare:

```
"BatchGetMetricData",
"ListRecommendations",
"CreateDeliverabilityTestReport",
"CreateEmailIdentityPolicy",
"DeleteEmailIdentity",
"DeleteEmailIdentityPolicy",
"GetDomainStatisticsReport",
"GetEmailIdentity",
"GetEmailIdentityPolicies",
"PutEmailIdentityConfigurationSetAttributes",
"PutEmailIdentityDkimAttributes",
"PutEmailIdentityDkimSigningAttributes",
"PutEmailIdentityFeedbackAttributes",
"PutEmailIdentityMailFromAttributes",
"TagResource",
"UntagResource",
"UpdateEmailIdentityPolicy"
```

Le policy di autorizzazione dell'identità consentono inoltre di limitare il principale a una sola di queste azioni.

```
{
  "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 di più istruzioni

La policy di autorizzazione dell'identità può includere più istruzioni. La policy di esempio seguente include due istruzioni. La prima istruzione impedisce a due utenti di accedere a `getemailidentity` da sender@example.com all'interno dello stesso account `123456789012`. La seconda istruzione nega `UpdateEmailIdentityPolicy` per il principale, Jack, all'interno dello stesso account `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"
      ]
    }
  ]
}
```

Gestione delle policy per l'autorizzazione dell'identità in Amazon SES

Oltre a creare le policy e a collegarle alle identità, è possibile modificare, rimuovere, elencare e recuperare le policy di un'identità, come descritto nelle sezioni seguenti.

Gestione di policy mediante la console Amazon SES

La gestione delle policy di Amazon SES comporta la visualizzazione, la modifica o l'eliminazione di una policy allegata a un'identità utilizzando la console Amazon SES.

Per gestire policy utilizzando la console Amazon SES

1. Accedi alla AWS Management Console e apri la console Amazon SES all'indirizzo https://console.aws.amazon.com/ses/.
2. Nel pannello di navigazione a sinistra, scegli Verified identities (Identità verificate).
3. Nell'elenco delle identità, scegli l'identità che vuoi gestire.
4. Nella pagina dei dettagli dell'identità, apri la scheda Authorization (Autorizzazione). Qui troverai un elenco di tutte le policy associate a questa identità.
5. Seleziona la policy che desideri gestire scegliendo la relativa casella di controllo.
6. A seconda dell'attività di gestione desiderata, scegliere il pulsante corrispondente come segue:

    a. Visualizzare una policy, scegli View policy (Visualizza policy). Se hai bisogno di una copia, scegli il pulsante Copy (Copia) per eseguire una copia negli appunti.

    b. Per modificare la policy, scegli Edit (Modifica). Nel riquadro Policy document (Documento policy), modifica la policy e scegli Save changes (Salva modifiche).

    > **Note**
    >
    > Per revocare le autorizzazioni, puoi modificare la policy o rimuoverla.

    c. Per rimuovere la policy, scegli Delete (Elimina).

> **Important**
>
> La rimozione di una policy è permanente. È consigliabile eseguire il backup della policy copiandola e incollandola in un file di testo prima di rimuoverla.

Gestione di policy mediante l'API Amazon SES

La gestione delle policy di Amazon SES comporta la visualizzazione, la modifica o l'eliminazione di una policy allegata a un'identità utilizzando l'API di Amazon SES.

Pubblicazione e visualizzazione delle policy tramite l'API Amazon SES

- È possibile visualizzare l'elenco delle policy collegate a un'identità usando l'operazione API ListIdentityPolicies. È inoltre possibile recuperare le policy usando l'operazione API GetIdentityPolicies.

Per modificare una policy usando l'API di Amazon SES

- Puoi modificare una policy collegata a un'identità utilizzando l'operazione API PutIdentityPolicy.

Per eliminare una policy usando l'API di Amazon SES

- Puoi eliminare una policy collegata a un'identità utilizzando l'operazione API DeleteIdentityPolicy.

Uso dell'autorizzazione di invio con Amazon SES

Puoi configurare Amazon SES per autorizzare altri utenti a inviare e-mail da identità di tua proprietà (domini o indirizzi e-mail) usando i loro account Amazon SES. Questa funzionalità, chiamata autorizzazione di invio, ti permette di mantenere il controllo sulle tue identità, in modo da poter modificare o revocare le autorizzazioni in qualsiasi momento. Ad esempio, un titolare di azienda può usare l'autorizzazione di invio per permettere a una terza parte, come una società di marketing via e-mail, di inviare e-mail da un dominio di sua proprietà.

In questo capitolo vengono descritte le specifiche dell'autorizzazione di invio che sostituisce la precedente funzionalità di notifica tra account. È necessario innanzitutto comprendere le basi dell'autorizzazione basata sull'identità utilizzando le policy di autorizzazione come descritto in Uso

dell'autorizzazione dell'identità in Amazon SES cui vengono illustrati argomenti importanti quali l'anatomia di una policy di autorizzazione e come gestire le policy.

Supporto legacy delle notifiche tra account

Generalmente, le notifiche di feedback per mancati recapiti, reclami e consegne di e-mail inviate da un mittente delegato, autorizzato dal proprietario dell'identità all'invio da una delle sue identità verificate, venivano configurate utilizzando notifiche tra account in cui il mittente delegato associava un argomento a un'identità non di sua proprietà (ecco perché "tra account"). Tuttavia, le notifiche tra account sono state sostituite utilizzando set di configurazione e identità verificate in associazione con l'invio del delegato in cui il mittente delegato è stato autorizzato dal proprietario dell'identità a utilizzare una delle proprie identità verificate per l'invio di e-mail. Questo nuovo metodo offre la flessibilità di configurare le notifiche di mancato recapito, reclamo, consegna e altri eventi mediante i due seguenti costrutti, a seconda che l'utente sia il mittente delegato o il proprietario dell'identità verificata:

- Set di configurazione: il mittente delegato può impostare la pubblicazione di eventi nel proprio set di configurazione, da specificare quando invia e-mail da un'identità verificata di cui non è in possesso, ma che è stato autorizzato a inviare dal proprietario dell'identità tramite una policy di autorizzazione. La pubblicazione di eventi consente di pubblicare notifiche di rimbalzo, reclamo, consegna e altri eventi su Amazon, CloudWatch Amazon Data Firehose, Amazon Pinpoint e Amazon SNS. Per informazioni, consulta Crea destinazioni degli eventi.
- Identità verificate: oltre a poter autorizzare il mittente delegato a utilizzare una delle sue identità verificate per l'invio di e-mail, con questo costrutto il proprietario dell'identità può, su richiesta del mittente delegato, configurare notifiche di feedback sull'identità condivisa in modo che utilizzino argomenti SNS di proprietà del mittente delegato. Solo il mittente delegato riceverà queste notifiche, perché è proprietario dell'argomento SNS. Per informazioni su come configurare un "SNS topic you don't own" ("Argomento SNS non in tuo possesso") nelle procedure della policy di autorizzazione, consulta il passaggio 14.

> **Note**
>
> Per compatibilità, le notifiche tra account sono supportate per le notifiche legacy tra account attualmente in uso nel tuo account. Tale supporto è limitato alla possibilità di modificare e utilizzare eventuali account incrociati correnti creati nella console classica di Amazon SES; tuttavia, non puoi più creare nuove notifiche tra account. Per crearne di nuove nella nuova console di Amazon SES, utilizza i nuovi metodi di invio tramite mittente delegato con set di

configurazione utilizzando la pubblicazione di eventi o con identità verificate configurate con i tuoi argomenti SNS.

Argomenti

Panoramica dell'autorizzazione di invio in Amazon SES

Questo argomento offre una panoramica del processo di autorizzazione di invio e descrive quindi il funzionamento delle caratteristiche di invio di e-mail in Amazon SES, tra cui le quote di invio e le notifiche, con l'autorizzazione di invio.

Questa sezione usa i termini seguenti:

- Identità: dominio o indirizzo e-mail usato dagli utenti di Amazon SES per inviare e-mail.
- Proprietario di identità: utente di Amazon SES che ha verificato la proprietà di un dominio o indirizzo e-mail usando le procedure descritte in Identità verificate.
- Mittente delegato: un account AWS, un utente AWS Identity and Access Management (IAM) o un servizio AWS autorizzato tramite una policy di autorizzazione a inviare e-mail per conto del proprietario dell'identità.
- Policy di autorizzazione di invio: documento da collegare a un'identità per specificare chi può inviare e-mail per l'identità e in quali condizioni.
- Amazon Resource Name (ARN): elemento standardizzato per identificare in modo univoco una risorsa AWS tra tutti i servizi AWS. Per l'autorizzazione all'invio, la risorsa è l'identità che il proprietario dell'identità ha autorizzato per l'utilizzo da parte del mittente delegato. Un esempio di ARN è arn:aws:ses:us-east-1:123456789012:identity/example.com.

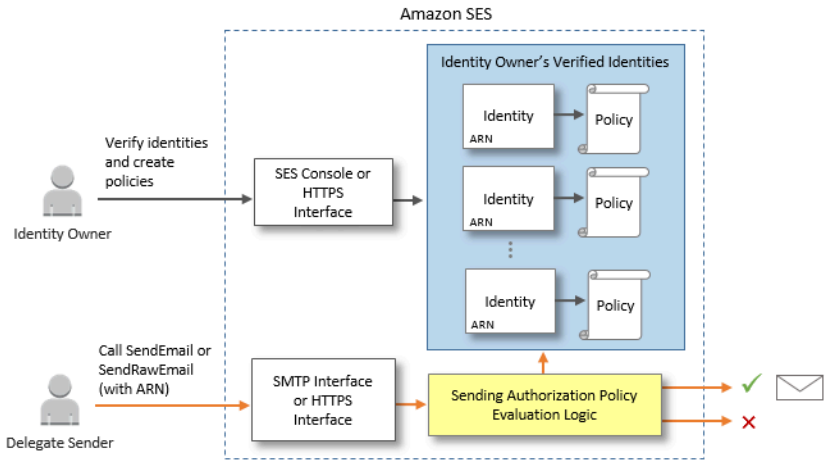
Processo di autorizzazione di invio

L'autorizzazione di invio si basa su policy di autorizzazione di invio. Se vuoi permettere a un mittente delegato di inviare e-mail per conto tuo, devi creare una policy di autorizzazione di invio e associare la policy alla tua identità usando la console oppure l'API Amazon SES. Quando il mittente delegato

tenta di inviare un'e-mail tramite Amazon SES per conto tuo, passa l'ARN della tua identità nella richiesta o nell'intestazione dell'e-mail.

Quando Amazon SES riceve la richiesta di invio dell'e-mail, controlla la policy della tua identità, se presente, per determinare se hai autorizzato il mittente delegato a inviare e-mail per conto dell'identità. Se il mittente delegato è autorizzato, Amazon SES accetta l'e-mail; in caso contrario, Amazon SES restituisce un messaggio di errore.

Il diagramma seguente mostra la relazione generale tra i concetti correlati all'autorizzazione di invio:



Il processo di autorizzazione di invio è costituito dalle fasi seguenti:

1. Il proprietario dell'identità seleziona un'identità verificata da utilizzare per il mittente delegato. (Se non disponi di un'identità e-mail verificata, consulta Identità verificate).

   > **Note**
   >
   > L'identità verificata scelta per il mittente delegato non può avere un set di configurazione predefinito assegnato.

2. Il mittente delegato comunica al proprietario dell'identità quale ID account AWS o ARN dell'utente IAM desidera utilizzare per l'invio.
3. Se il proprietario dell'identità accetta di consentire al mittente delegato di inviare da uno dei propri account, egli crea una policy di autorizzazione di invio e collega la policy all'identità scelta usando la console Amazon SES o l'API Amazon SES.

4. Il proprietario dell'identità fornisce al mittente delegato l'ARN dell'identità autorizzata, in modo che questi possa a sua volta fornire l'ARN ad Amazon SES al momento dell'invio dell'e-mail.
5. Il mittente delegato può configurare le notifiche di mancato recapito e reclamo tramite la pubblicazione degli eventi abilitata in un set di configurazione specificato durante l'invio tramite mittente delegato. Il proprietario dell'identità può anche configurare le notifiche e-mail di feedback per eventi di mancato recapito e reclamo da inviare agli argomenti Amazon SNS del mittente delegato.

> **Note**
>
> Se il proprietario dell'identità disabilita l'invio di notifiche di eventi, il mittente delegato deve configurare la pubblicazione degli eventi per pubblicare gli eventi di rimbalzo e reclamo su un argomento di Amazon SNS o uno stream Firehose. Il mittente deve anche applicare il set di configurazione che contiene la regola di pubblicazione dell'evento a ogni e-mail inviata. Se né il proprietario di identità né il mittente delegato impostano un metodo di invio delle notifiche relative a eventi di mancato recapito e reclamo, Amazon SES invia automaticamente le notifiche di eventi tramite e-mail all'indirizzo indicato nel percorso di ritorno dell'e-mail (o l'indirizzo nel campo dell'origine, se non hai specificato un indirizzo per il percorso di ritorno), anche se il proprietario di identità ha disabilitato l'inoltro di feedback via e-mail.

6. Il mittente delegato tenta di inviare un'e-mail tramite Amazon SES per conto del proprietario di identità passando l'ARN dell'identità del proprietario di identità nella richiesta o nell'intestazione dell'e-mail. Il mittente delegato può inviare l'e-mail usando l'interfaccia SMTP o l'API Amazon SES. Alla ricezione della richiesta, Amazon SES esamina tutte le policy collegate all'identità e accetta l'e-mail se il mittente delegato è autorizzato a usare l'indirizzo del mittente specificato e l'indirizzo del percorso di ritorno. In caso contrario, Amazon SES restituisce un errore e non accetta il messaggio.

> **Important**
>
> L'account AWS del mittente delegato deve essere rimosso dall'ambiente di sperimentazione (sandbox) prima che possa essere utilizzato per inviare e-mail a indirizzi non verificati.

7. Per annullare l'autorizzazione dell'identità del mittente delegato, il proprietario di identità modifica semplicemente la policy di autorizzazione di invio o la elimina completamente. Il proprietario di identità è in grado di eseguire entrambe le azioni utilizzando la console o l'API Amazon SES.

Per ulteriori informazioni sul modo in cui il proprietario di identità o il mittente delegato esegue queste attività, consulta rispettivamente Attività del proprietario di identità o Attività del mittente delegato.

Attribuzione delle funzionalità di invio di e-mail

È importante comprendere il ruolo del mittente delegato e del proprietario di identità relativamente alle funzionalità di invio di e-mail di Amazon SES, come la quota di invio giornaliera, i mancati recapiti e i reclami, la firma DKIM, l'inoltro di feedback e così via. L'attribuzione riguarda gli aspetti seguenti:

- Quote di invio: le e-mail inviate dalle identità del proprietario di identità vengono conteggiate rispetto alle quote del mittente delegato.
- Mancati recapiti e reclami: gli eventi di mancato recapito e reclamo vengono registrati nell'account Amazon SES del mittente delegato e, di conseguenza, possono influire sulla reputazione del mittente delegato.
- Firma DKIM: se il proprietario di identità ha abilitato la firma Easy DKIM per un'identità, tutte le e-mail inviate da questa identità saranno provviste di firma DKIM, incluse le e-mail inviate dal mittente delegato. Solo il proprietario di identità può controllare se le e-mail debbano o meno essere provviste di firma DKIM.
- Notifiche: il proprietario di identità e il mittente delegato possono entrambi configurare le proprie notifiche per mancati recapiti e reclami. Il proprietario di identità dell'indirizzo e-mail può anche attivare l'inoltro di feedback via e-mail. Per informazioni sulla configurazione delle notifiche, consulta Monitoraggio delle attività di invio di Amazon SES.
- Verifica: i proprietari di identità sono responsabili dell'applicazione della procedura descritta in Identità verificate per verificare di essere i proprietari dei domini e degli indirizzi e-mail per il cui uso intendono autorizzare i mittenti delegati. I mittenti delegati non devono verificare alcun dominio o indirizzo e-mail espressamente per l'autorizzazione di invio.

> **Important**
>
> L'account AWS del mittente delegato deve essere rimosso dall'ambiente di sperimentazione (sandbox) prima che possa essere utilizzato per inviare e-mail a indirizzi non verificati.

- Regioni AWS: il mittente delegato deve inviare le e-mail dalla regione AWS in cui viene verificata l'identità del proprietario di identità. La policy di autorizzazione di invio che concede l'autorizzazione al mittente delegato deve essere collegata all'identità in questa regione.
- Fatturazione: tutti i messaggi inviati dall'account del mittente delegato, comprese le e-mail che il mittente delegato invia utilizzando gli indirizzi del proprietario di identità, vengono fatturate per il mittente delegato.

Attività del proprietario di identità per l'autorizzazione di invio di Amazon SES

In questa sezione vengono descritte le fasi che i proprietari di identità devono seguire per configurare l'autorizzazione di invio.

Argomenti

Verifica di un'identità per l'autorizzazione di invio di Amazon SES

La prima fase per configurare l'autorizzazione di invio consiste nel dimostrare di essere il proprietario del dominio o dell'indirizzo e-mail utilizzato dal mittente delegato per e-mail. La procedura di verifica è descritta in Identità verificate.

Puoi confermare che un indirizzo e-mail o un dominio sia verificato esaminandone lo stato nella sezione Verified Identities (Identità verificate) della https://console.aws.amazon.com/ses/ oppure con l'operazione API `GetIdentityVerificationAttributes`.

Prima che l'utente o il mittente delegato possa inviare e-mail a indirizzi e-mail non verificati, occorre inviare una richiesta affinché l'account venga rimosso dalla sandbox Amazon SES. Per ulteriori informazioni, consultare Richiedi l'accesso alla produzione (uscita dalla sandbox di Amazon SES).

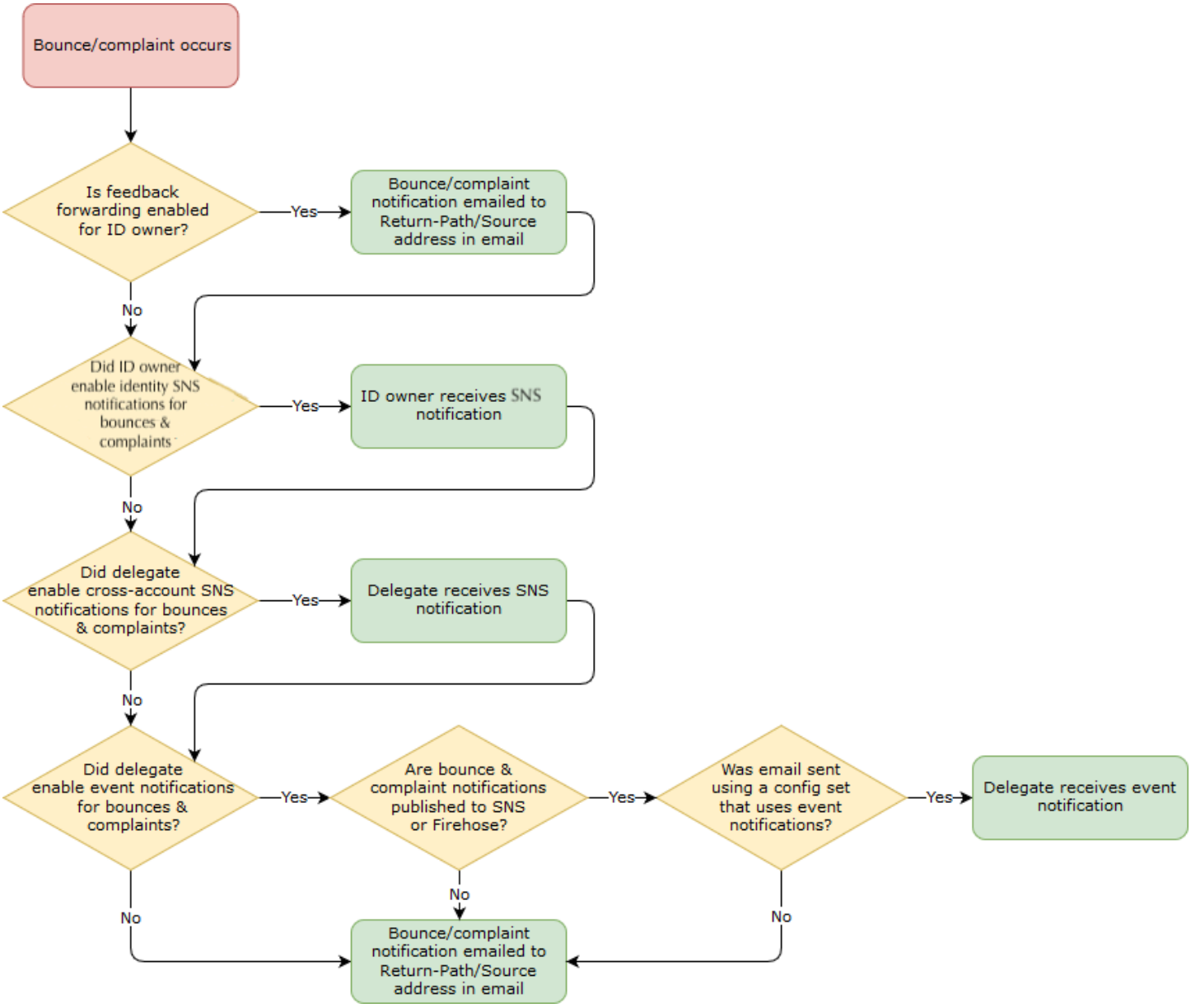
> **Important**
>
> L'Account AWS del mittente delegato deve essere rimosso dalla sandbox prima che possa essere utilizzato per inviare e-mail a indirizzi non verificati.

Impostazione delle notifiche del proprietario di identità per l'autorizzazione di invio di Amazon SES

Se autorizzi un mittente delegato a inviare e-mail a tuo nome, i messaggi di mancato recapito e reclamo generati da tali e-mail vengono conteggiati da Amazon SES nei parametri relativi ai messaggi di mancato recapito e reclamo del delegato e non tuoi. Tuttavia, se il tuo indirizzo IP è visualizzato su DNSBL (DNS-based Blackhole Lists) anti-spam di terze parti a causa di messaggi inviati da un mittente delegato, la reputazione delle tue identità potrebbe essere compromessa. Per questo motivo, se sei un proprietario di identità, ti consigliamo di impostare l'inoltro di feedback via e-mail per la tue identità, incluse quelle che hai autorizzato per l'invio dei delegati. Per ulteriori informazioni, consulta Ricezione delle notifiche Amazon SES tramite e-mail.

I mittenti delegati possono e devono configurare le notifiche di mancato recapito e reclamo per le identità che li hai autorizzati ad usare. Possono configurare la pubblicazione di eventi per pubblicare eventi di rimbalzo e reclamo su un argomento di Amazon SNS o uno stream Firehose.

Se né il proprietario di identità né il mittente delegato imposta un metodo di invio delle notifiche relative a eventi di mancato recapito e reclamo o se il mittente non applica il set di configurazione che utilizza la regola di pubblicazione degli eventi, Amazon SES invia automaticamente le notifiche di eventi tramite e-mail all'indirizzo indicato nel percorso di ritorno dell'e-mail (o all'indirizzo nel campo dell'origine, se non hai specificato un indirizzo per il percorso di ritorno), anche se hai disabilitato l'inoltro di feedback via e-mail. Questo processo è illustrato nell'immagine seguente.



Recupero di informazioni dal mittente delegato per l'autorizzazione di invio di Amazon SES

La policy di autorizzazione dell'invio deve specificare almeno un'entità principale, che è l'entità del mittente delegato a cui stai concedendo l'accesso in modo che possa inviare e-mail per conto di una delle tue identità verificate. Per le policy di autorizzazione di invio di Amazon SES, il principale può essere l'account AWS del tuo mittente delegato, l'ARN del utente (IAM) AWS Identity and Access Management o un servizio AWS.

Per maggiore semplicità, puoi considerare l'entità principale (mittente delegato) come beneficiario e te stesso (proprietario dell'identità) come il garante della policy con cui cui concedi l'autorizzazione

Enable (Abilita) a inviare qualsiasi combinazione di e-mail, e-mail in formato RAW, e-mail con modelli o e-mail con modelli in blocco dalla risorsa (identità verificata) di tua proprietà.

Se desideri ottenere il controllo più granulare, chiedi al mittente delegato di configurare un utente IAM, in modo che solo un mittente delegato possa eseguire l'invio per tuo conto, anziché qualsiasi utente nell'account AWS del mittente delegato. Il mittente delegato può trovare informazioni sulla configurazione di un utente IAM nella pagina relativa alla creazione di un utente IAM nell'account AWS nella Guida per l'utente di IAM.

Chiedi l'ID dell'account AWS o l'Amazon Resource Name (ARN) dell'utente IAM al mittente delegato, in modo da poterlo includere nella tua policy di autorizzazione all'invio. Consiglia al mittente delegato di seguire le istruzioni per trovare queste informazioni in Inoltro delle informazioni al proprietario di identità. Se il mittente delegato è un servizio AWS, consulta la documentazione per il servizio per determinare il relativo nome.

La seguente policy di esempio illustra gli elementi di base necessari in una policy creata dal proprietario dell'identità per autorizzare il mittente delegato all'invio dalla risorsa del proprietario dell'identità. È necessario che il proprietario dell'identità acceda al flusso di lavoro Verified identities (Identità verificate) e, in Autorizzazione, utilizzi il generatore di policy per creare, nella sua forma più semplice, la policy di base seguente che autorizza il mittente delegato all'invio per conto di una risorsa di proprietà del proprietario dell'identità:

```
{
    "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": {}
        }
    ]
}
```

La legenda seguente spiega gli elementi chiave della policy riportata sopra e chi li possiede:

- Principal (Entità principale): questo campo è compilato con l'ARN dell'utente IAM del mittente delegato.
- Action (Operazione): questo campo è popolato con due azioni SES (`SendEmail` e `SendRawEmail`) che il proprietario dell'identità autorizza il mittente delegato a eseguire dalla risorsa del proprietario dell'identità.
- Resource (Risorsa): questo campo è popolato con la risorsa verificata del proprietario dell'identità da cui il mittente delegato è autorizzato a inviare e-mail.

Creazione di una policy per l'autorizzazione all'invio di Amazon SES

In maniera simile alla creazione di una policy di autorizzazione in Amazon SES, come spiegato in Creazione di una policy di autorizzazione identità, per autorizzare un mittente delegato a inviare e-mail utilizzando un indirizzo e-mail o un dominio (un'identità) di tua proprietà, devi creare la policy con azioni API di invio SES specificate e quindi collegare tale policy all'identità.

Per un elenco delle azioni API che possono essere specificate in una policy di autorizzazione di invio, consulta la riga Azione nella tabella the section called “Istruzioni specifiche della policy”.

Puoi creare una policy di autorizzazione di invio utilizzando il generatore di policy o creando una policy personalizzata. Procedure specifiche per la creazione di una policy di autorizzazione di invio sono fornite per entrambi i metodi.

> **Note**
>
> - Le policy di autorizzazione di invio che colleghi alle identità degli indirizzi e-mail hanno la precedenza sulle policy collegate alle identità di dominio corrispondenti. Ad esempio, se crei una policy per esempio.com che non autorizza un mittente delegato e crei una policy per mittente@esempio.com che autorizza il mittente delegato, quest'ultimo può inviare e-mail da mittente@esempio.com, ma non da qualsiasi altro indirizzo nel dominio esempio.com.
> - Se crei una policy per esempio.com che autorizza un mittente delegato e crei una policy per mittente@esempio.com che non autorizza il mittente delegato, il mittente delegato può inviare e-mail da qualsiasi indirizzo nel dominio esempio.com ad eccezione di mittente@esempio.com.
> - Se non hai familiarità con la struttura delle policy di autorizzazione SES, consulta Anatomia delle policy.

Creazione di una policy di autorizzazione di invio tramite il generatore di policy

Puoi usare il generatore di policy per creare una semplice policy di autorizzazione di invio seguendo i passaggi indicati.

Per creare una policy di autorizzazione di invio tramite il generatore di policy

1. Accedi alla AWS Management Console e apri la console Amazon SES all'indirizzo https://console.aws.amazon.com/ses/.
2. Nel pannello di navigazione, in Configuration (Configurazione), scegli Verified identities (Identità verificate).
3. Nel container Identities (Identità) della schermata Verified identities (Identità verificate), seleziona l'identità verificata tramite cui desideri che il mittente delegato sia autorizzato a inviare e-mail per conto tuo.
4. Scegli la scheda Autorizzazione dell'identità verificata.
5. Nel riquadro Authorization policies (Policy di autorizzazione), scegli Create policy (Crea policy) e seleziona Use policy generator (Usa generatore di policy) dal menu a discesa.
6. Nel riquadro Create statement (Crea istruzione), scegli Allow (Consenti) nel campo Effect (Effetto). Se invece desideri creare una policy per negare l'autorizzazione al mittente delegato, scegli Deny (NEGA).
7. Nel campo Principals (Entità principali), inserisci l'ID Account AWS o l'ARN dell'utente IAM che il mittente delegato ha condiviso con te per essere autorizzato a inviare e-mail per conto del tuo account da questa identità, quindi scegli Add (Aggiungi). Se desideri autorizzare più mittenti delegati, ripeti questo passaggio per ognuno di questi.
8. Nel campo Actions (Operazioni), seleziona la casella di controllo per ogni tipo di invio che desideri autorizzare da parte del mittente delegato.
9. (Facoltativo) Espandi Specify conditions (Specifica condizioni) se desideri aggiungere un'istruzione di qualificazione all'autorizzazione del mittente delegato.
    a. Seleziona un operatore dal menu a discesa Operator (Operatore).
    b. Seleziona un tipo di chiave dal menu a discesa Key (Chiave).
    c. In base al tipo di chiave selezionato, inserisci il valore corrispondente nel campo Value (Valore). Se desideri aggiungere altre condizioni, scegli Add new condition (Aggiungi nuova condizione) e ripeti questo passaggio per ciascuna di esse.
10. Scegli Save statement (Salva istruzione).

11. (Facoltativo) Se desideri aggiungere altre istruzioni alla tua policy, espandi Create another statement (Crea un'altra istruzione) e ripeti i passaggi da 6 a 10.
12. Scegli Next (Successivo) e nella schermata Customize policy (Personalizza policy), il container Edit policy details (Modifica dettagli policy) dispone di campi in cui puoi modificare o personalizzare le voci Name (Nome) e Policy document (Documento policy).
13. Scegli Next (Successivo) e nella schermata Review and apply (Rivedi e applica) il container Overview (Panoramica) mostrerà l'identità verificata che stai autorizzando per il mittente delegato e il nome di questa policy. Nel riquadro Policy document (Documento policy) sarà presente la policy effettiva che hai appena scritto insieme a tutte le condizioni che hai aggiunto: controlla la policy e, se sembra corretta, scegli Apply policy (Applica policy). Se hai bisogno di modificare o correggere qualcosa, scegli Previous (Precedente) e lavora nel container Edit policy details (Modifica dettagli policy). La policy appena creata consentirà al mittente delegato di inviare per tuo conto.
14. (Facoltativo) Se il mittente delegato desidera utilizzare anche un argomento SNS di cui è proprietario, per ricevere notifiche di feedback quando riceve mancati recapiti o reclami o quando le e-mail vengono consegnate, dovrai configurare il relativo argomento SNS in questa identità verificata. Il mittente delegato dovrà condividere con te il proprio ARN dell'argomento SNS. Seleziona la scheda Notifications (Notifiche) e scegli Edit (Modifica) nel container Feedback notifications (Notifiche feedback):

    a. Nel riquadro Configure SNS topics (Configura argomenti SNS), in uno dei campi di feedback (Bounce (Mancato recapito), Complaint (Reclamo) o Delivery (Consegna)) seleziona SNS topic you don’t own (Argomento SNS non di tua proprietà) e inserisci l'SNS topic ARN (ARN dell'argomento SNS) di proprietà e condiviso con te dal mittente delegato. Solo il mittente delegato riceverà queste notifiche, perché possiede l'argomento SNS: tu, in quanto proprietario dell'identità, no.

    b. (Facoltativo) Se desideri che la notifica dell'argomento includa le intestazioni dall'e-mail originale, seleziona la casella Include original email headers (Includi intestazioni e-mail originali) direttamente sotto il nome dell'argomento SNS di ogni tipo di feedback. Questa opzione è disponibile solo se hai assegnato un argomento Amazon SNS al tipo di notifica associato. Per informazioni sui contenuti delle intestazioni e-mail originali, consulta l'oggetto `mail` in Contenuti delle notifiche.

    c. Seleziona Salva modifiche. Potrebbero essere necessari alcuni minuti perché le modifiche apportate alle impostazioni di notifica diventino effettive.

d. (Facoltativo) Poiché il mittente delegato riceverà notifiche sull'argomento Amazon SNS per mancati recapiti e reclami, puoi disabilitare completamente le notifiche via e-mail se non desideri ricevere feedback per gli invii di questa identità. Per disabilitare le notifiche e-mail per mancati recapiti e reclami, sotto la scheda Notifications (Notifiche), nel container Email Feedback Forwarding (Inoltro feedback e-mail), scegli Edit (Modifica), deseleziona la casella Enabled (Abilitato) e scegli Save changes (Salva modifiche). Le notifiche sullo stato della consegna ora verranno inviate solo agli argomenti SNS di proprietà del mittente delegato.

Creazione di una policy di autorizzazione di invio personalizzata

Se desideri creare una policy di autorizzazione di invio personalizzata e collegarla a un'identità, hai a disposizione le seguenti opzioni:

- Uso dell'API Amazon SES: puoi creare una policy in un editor di testo, quindi collegarla all'identità usando l'API `PutIdentityPolicy` descritta nella Documentazione di riferimento per le API Amazon Simple Email Service.
- Uso della console Amazon SES: puoi creare una policy in un editor di testo e collegarla a un'identità incollandola nell'editor di policy personalizzate nella console Amazon SES. Questo metodo viene descritto nella procedura seguente.

Per creare una policy di autorizzazione di invio personalizzata usando l'editor di policy personalizzate

1. Accedi alla AWS Management Console e apri la console Amazon SES all'indirizzo https://console.aws.amazon.com/ses/.
2. Nel pannello di navigazione, in Configuration (Configurazione), scegli Verified identities (Identità verificate).
3. Nel container Identities (Identità) della schermata Verified identities (Identità verificate), seleziona l'identità verificata tramite cui desideri che il mittente delegato sia autorizzato a inviare e-mail per conto tuo.
4. Nella schermata dei dettagli dell'identità verificata selezionata nel passaggio precedente, scegli la scheda Authorization (Autorizzazione).
5. Nel riquadro Authorization policies (Policy di autorizzazione), scegli Create policy (Crea policy) e seleziona Create custom policy (Crea policy personalizzata) dal menu a discesa.

6. Nel riquadro Policy document (Documento policy), digita o incolla il testo della policy nel formato JSON. Puoi anche usare il generatore di policy per creare rapidamente la struttura di base di una policy e personalizzarla qui.
7. Scegli Apply Policy (Applica policy). Se hai bisogno di modificare la policy personalizzata, seleziona la relativa casella di controllo sotto la scheda Authorization (Autorizzazione), scegli Edit (Modifica) e apporta le modifiche nel riquadro Policy document (Documento policy) seguito da Save changes (Salva modifiche).
8. (Facoltativo) Se il mittente delegato desidera utilizzare anche un argomento SNS di cui è proprietario, per ricevere notifiche di feedback quando riceve mancati recapiti o reclami o quando le e-mail vengono consegnate, dovrai configurare il relativo argomento SNS in questa identità verificata. Il mittente delegato dovrà condividere con te il proprio ARN dell'argomento SNS. Seleziona la scheda Notifications (Notifiche) e scegli Edit (Modifica) nel container Feedback notifications (Notifiche feedback):

    a. Nel riquadro Configure SNS topics (Configura argomenti SNS), in uno dei campi di feedback (Bounce (Mancato recapito), Complaint (Reclamo) o Delivery (Consegna)) seleziona SNS topic you don’t own (Argomento SNS non di tua proprietà) e inserisci l'SNS topic ARN (ARN dell'argomento SNS) di proprietà e condiviso con te dal mittente delegato. Solo il mittente delegato riceverà queste notifiche, perché possiede l'argomento SNS: tu, in quanto proprietario dell'identità, no.

    b. (Facoltativo) Se desideri che la notifica dell'argomento includa le intestazioni dall'e-mail originale, seleziona la casella Include original email headers (Includi intestazioni e-mail originali) direttamente sotto il nome dell'argomento SNS di ogni tipo di feedback. Questa opzione è disponibile solo se hai assegnato un argomento Amazon SNS al tipo di notifica associato. Per informazioni sui contenuti delle intestazioni e-mail originali, consulta l'oggetto `mail` in Contenuti delle notifiche.

    c. Seleziona Salva modifiche. Potrebbero essere necessari alcuni minuti perché le modifiche apportate alle impostazioni di notifica diventino effettive.

    d. (Facoltativo) Poiché il mittente delegato riceverà notifiche sull'argomento Amazon SNS per mancati recapiti e reclami, puoi disabilitare completamente le notifiche via e-mail se non desideri ricevere feedback per gli invii di questa identità. Per disabilitare le notifiche e-mail per mancati recapiti e reclami, sotto la scheda Notifications (Notifiche), nel container Email Feedback Forwarding (Inoltro feedback e-mail), scegli Edit (Modifica), deseleziona la casella Enabled (Abilitato) e scegli Save changes (Salva modifiche). Le notifiche sullo stato della consegna ora verranno inviate solo agli argomenti SNS di proprietà del mittente delegato.

Esempi di policy di invio

L'autorizzazione di invio ti permette di specificare le condizioni granulari in base alle quali permettere ai mittenti delegati di inviare e-mail per conto tuo.

Gli esempi e le condizioni seguenti mostrano come scrivere policy per controllare diversi aspetti dell'invio:

- Condizioni specifiche per l'autorizzazione di invio
- Definizione del mittente delegato
- Limitazione dell'indirizzo del mittente
- Limitazione dei momenti in cui il delegato può inviare e-mail
- Limitazione dell'operazione di invio di e-mail
- Limitazione del nome visualizzato del mittente dell'e-mail
- Uso di più istruzioni

Condizioni specifiche per l'autorizzazione di invio

Una condizione è qualsiasi restrizione riguardo all'autorizzazione inclusa nell'istruzione. La parte dell'istruzione che specifica le condizioni può essere la più dettagliata di tutte le parti. Una chiave è la caratteristica specifica sui cui si basa la restrizione di accesso, ad esempio la data e l'ora della richiesta.

Usa insieme condizioni e chiavi per esprimere la limitazione. Ad esempio, se vuoi impedire al mittente delegato di inviare richieste ad Amazon SES per tuo conto dopo il 30 luglio 2019, devi usare la condizione denominata `DateLessThan`. Usi la chiave denominata `aws:CurrentTime` e la imposti sul valore `2019-07-30T00:00:00Z`.

Puoi usare una qualsiasi delle chiavi specifiche di AWS elencate nella sezione relativa alle chiavi disponibili della Guida per l'utente di IAM oppure puoi usare una delle chiavi seguenti specifiche di SES che sono utili nell'invio di policy di autorizzazione:

Chiave di condizione	Descrizione
`ses:Recipients`	Limita gli indirizzi del destinatario, che includono gli indirizzi "A", "CC" e "CCN".

Chiave di condizione	Descrizione
`ses:FromAddress`	Limita l'indirizzo "From".
`ses:FromDisplayName`	Limita il contenuto della stringa usata come nome visualizzato del mittente, a volte chiamato "friendly from". Ad esempio, il nome visualizzato di "John Doe <johndoe@example.com>" è John Doe.
`ses:FeedbackAddress`	Limita l'indirizzo "percorso di ritorno", ovvero l'indirizzo a cui ti possono essere inviati reclami e notifiche di mancato recapito tramite l'inoltro di feedback via e-mail. Per informazioni sull'inoltro di feedback via e-mail, consulta Ricezione delle notifiche Amazon SES tramite e-mail.

Puoi utilizzare le condizioni `StringEquals` e `StringLike` con le chiavi Amazon SES. Queste condizioni sono per la corrispondenza di stringhe con distinzione tra maiuscole e minuscole. In `StringLike`, i valori possono includere una corrispondenza con più caratteri jolly (*) o con un singolo carattere jolly (?) ovunque nella stringa. Ad esempio, la condizione seguente specifica che il mittente delegato può inviare e-mail solo da un indirizzo che inizia con invoicing e termina con @example.com:

```
"Condition": {
    "StringLike": {
      "ses:FromAddress": "invoicing*@example.com"
    }
}
```

Puoi anche utilizzare la condizione `StringNotLike` per impedire ai mittenti delegati di inviare e-mail da determinati indirizzi e-mail. Ad esempio, puoi non consentire l'invio da admin@example.com e da indirizzi simili, ad esempio "admin"@example.com, admin+1@example.com o sender@admin.example.com, includendo la condizione seguente nell'istruzione della policy:

```
"Condition": {
    "StringNotLike": {
      "ses:FromAddress": "*admin*example.com"
```

```
    }
 }
```

Per ulteriori informazioni su come specificare le condizioni, consulta Elementi delle policy JSON IAM: Condizioni nella Guida per l'utente di IAM.

Definizione del mittente delegato

L'entità principale, ossia l'entità cui concedi l'autorizzazione, può essere un Account AWS, un utente AWS Identity and Access Management (IAM) o un servizio AWS.

L'esempio seguente mostra una semplice policy che permette all'ID AWS 123456789012 di inviare e-mail dall'identità verificata example.com (di proprietà dell'account Account AWS 888888888888). L'istruzione `Condition` in questa policy autorizza solo il delegato (ossia, l'ID AWS 123456789012) a inviare e-mail dall'indirizzo marketing+.*@example.com, in cui * è una stringa che il mittente desidera aggiungere dopo 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 policy di esempio seguente concede a due utenti di IAM; l'autorizzazione necessaria per inviare e-mail dall'identità example.com. Gli utenti IAM vengono specificati tramite il rispettivo Amazon Resource Name (ARN).

```
{
  "Id":"ExampleAuthorizationPolicy",
  "Version":"2012-10-17",
  "Statement":[
    {
      "Sid":"AuthorizeIAMUser",
      "Effect":"Allow",
      "Resource":"arn:aws:ses:us-east-1:888888888888:identity/example.com",
      "Principal":{
        "AWS":[
          "arn:aws:iam::111122223333:user/John",
          "arn:aws:iam::444455556666:user/Jane"
        ]
      },
      "Action":[
        "ses:SendEmail",
        "ses:SendRawEmail"
      ]
    }
  ]
}
```

La policy di esempio seguente concede ad Amazon Cognito l'autorizzazione necessaria per inviare e-mail dall'identità 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 policy di esempio seguente concede a tutti gli account all'interno di un'Organizzazione AWS l'autorizzazione necessaria per inviare e-mail dall'identità example.com. L'organizzazione AWS viene specificata utilizzando la chiave di condizione globale PrincipalOrgID.

```
{
  "Id":"ExampleAuthorizationPolicy",
  "Version":"2012-10-17",
  "Statement":[
    {
      "Sid":"AuthorizeOrg",
      "Effect":"Allow",
      "Resource":"arn:aws:ses:us-east-1:888888888888:identity/example.com",
      "Principal":"*",
      "Action":[
        "ses:SendEmail",
        "ses:SendRawEmail"
      ],
      "Condition":{
        "StringEquals":{
          "aws:PrincipalOrgID":"o-xxxxxxxxxx"
        }
      }
    }
  ]
}
```

Limitazione dell'indirizzo del mittente

Se usi un dominio verificato, puoi creare una policy che permette solo al mittente delegato di inviare e-mail da un indirizzo e-mail specificato. Per limitare l'indirizzo del mittente, puoi impostare una condizione nella chiave denominata ses:FromAddress. La policy seguente permette all'ID Account AWS 123456789012 di inviare e-mail dall'identità example.com, ma solo dall'indirizzo e-mail sender@example.com.

```
{
  "Id":"ExamplePolicy",
  "Version":"2012-10-17",
  "Statement":[
    {
      "Sid":"AuthorizeFromAddress",
      "Effect":"Allow",
      "Resource":"arn:aws:ses:us-east-1:888888888888:identity/example.com",
      "Principal":{
        "AWS":[
          "123456789012"
        ]
      },
      "Action":[
        "ses:SendEmail",
        "ses:SendRawEmail"
      ],
      "Condition":{
        "StringEquals":{
          "ses:FromAddress":"sender@example.com"
        }
      }
    }
  ]
}
```

Limitazione dei momenti in cui il delegato può inviare e-mail

Puoi configurare la policy di autorizzazione di invio anche in modo tale che un mittente delegato possa inviare e-mail solo in certe ore del giorno o all'interno di un determinato intervallo di date. Ad esempio, se prevedi di creare una campagna e-mail durante il mese di settembre 2021, puoi usare la policy seguente per limitare la capacità del delegato all'invio di e-mail solo in quel mese.

```
{
```

```
  "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"
        }
      }
    }
  ]
}
```

Limitazione dell'operazione di invio di e-mail

Le operazioni che i mittenti possono usare per inviare un'e-mail con Amazon SES sono due: `SendEmail` e `SendRawEmail`, a seconda del livello di controllo che il mittente vuole avere sul formato dell'e-mail. Le policy di autorizzazione di invio permettono di limitare il mittente delegato a una di queste due operazioni. Tuttavia, molti proprietari di identità lasciano la scelta dei dettagli delle chiamate di invio di e-mail al mittente delegato, permettendo entrambe le operazioni nelle policy.

> **Note**
>
> Se vuoi permettere al mittente delegato di accedere ad Amazon SES tramite l'interfaccia SMTP, devi scegliere almeno `SendRawEmail`.

Se il tuo caso d'uso è tale da voler limitare l'operazione, a questo scopo puoi includere solo una delle operazioni nella policy di autorizzazione di invio. L'esempio seguente mostra come limitare l'operazione 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"
      ]
    }
  ]
}
```

Limitazione del nome visualizzato del mittente dell'e-mail

Alcuni client di posta elettronica visualizzano il nome "semplice" del mittente, se specificato nell'intestazione e-mail, invece dell'effettivo indirizzo del mittente. Ad esempio, il nome visualizzato di "John Doe <johndoe@example.com>" è John Doe. Ad esempio, puoi inviare e-mail da utente@esempio.com, ma scegliere che i destinatari vedano l'e-mail provenire da Marketing anziché da utente@esempio.com. La policy seguente permette all'ID Account AWS 123456789012 di inviare e-mail dall'identità example.com, ma solo se il nome visualizzato dell'indirizzo del mittente include 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 di più istruzioni

La policy di autorizzazione di invio può includere più istruzioni. La policy di esempio seguente include due istruzioni. La prima istruzione autorizza due Account AWS a inviare e-mail da sender@example.com, purché l'indirizzo del mittente e quello per il feedback usino entrambi il dominio example.com. La seconda istruzione autorizza un utente IAM a inviare e-mail da sender@example.com, purché l'indirizzo e-mail del destinatario faccia parte del 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"
        }
      }
    }
  ]
}
```

Inoltro al mittente delegato delle informazioni sull'identità per l'autorizzazione di invio di Amazon SES

Dopo aver creato la policy di autorizzazione di invio e averla collegata all'identità, è possibile fornire al mittente delegato l'Amazon Resource Name (ARN) dell'identità. Il mittente delegato passerà l'ARN ad Amazon SES nelle operazioni di invio di e-mail o nell'intestazione dell'e-mail. Per trovare l'ARN dell'identità, segui questa procedura.

Individuazione dell'ARN di un'identità

1. Accedere alla AWS Management Console e aprire la console Amazon SES all'indirizzo https://console.aws.amazon.com/ses/.
2. Nel pannello di navigazione, in Configuration (Configurazione), scegli Verified identities (Identità verificate).

3. Nell'elenco delle identità scegli l'identità a cui hai collegato la policy di autorizzazione di invio.
4. Nel riquadro Summary (Riepilogo), la seconda colonna, Amazon Resource Name (ARN), conterrà l'ARN dell'identità. Somiglierà al seguente: arn:aws:ses:us-east-1:123456789012:identity/user@example.com. Copia l'intero ARN e inoltralo al mittente delegato.

Attività del mittente delegato per l'autorizzazione all'invio di Amazon SES

Come mittente delegato, invii e-mail per conto di un'identità che non è di tua proprietà, ma che sei autorizzato a utilizzare. Anche se invii per conto del proprietario di identità, i mancati recapiti e i reclami sono conteggiati nei parametri relativi dell'account AWS e il numero di messaggi inviati viene conteggiato ai fini della quota di invio. Hai anche la responsabilità di richiedere qualsiasi aumento delle quote di invio che potrebbe essere necessario per inviare le e-mail del proprietario di identità.

In quanto mittente delegato, è necessario che completi le attività seguenti:

- Inoltro delle informazioni al proprietario di identità
- Utilizzo delle notifiche del mittente delegato
- Invio di e-mail per conto del proprietario di identità

Inoltro al proprietario di identità delle informazioni per l'autorizzazione all'invio di Amazon SES

In quanto mittente delegato, devi fornire al proprietario di identità l'ID account AWS o l'Amazon Resource Name (ARN) dell'utente IAM, poiché invierai e-mail per conto del proprietario dell'identità. Il proprietario dell'identità ha bisogno delle informazioni del tuo account, in modo da poter creare una policy che ti conceda il permesso di inviare da una delle sue identità verificate.

Se desideri utilizzare i tuoi argomenti SNS, puoi richiedere al proprietario dell'identità di configurare le notifiche di feedback per mancati recapiti, reclami o consegne da inviare a uno o più argomenti SNS. In questo modo, dovrai condividere il tuo ARN dell'argomento SNS con il proprietario dell'identità, in modo che possa configurare il tuo argomento SNS nell'identità verificata da cui ti autorizza a inviare.

Le seguenti procedure spiegano come trovare le informazioni dell'account e gli ARN dell'argomento SNS da condividere con il proprietario dell'identità.

Ricerca del tuo ID account AWS

1. Accedi all'AWS Management Console all'indirizzo https://console.aws.amazon.com.

2. Nell'angolo superiore destro della console, espandi il nome o il numero dell'account, quindi scegli My Account (Il mio account) nell'elenco a discesa.
3. La pagina Account settings (Impostazioni account) si aprirà e visualizzerà tutte le informazioni del tuo account, incluso il tuo ID dell'account AWS.

Per trovare l'ARN dell'utente IAM

1. Accedi all'AWS Management Console e apri la console IAM all'indirizzo https://console.aws.amazon.com/iam/.
2. Nel pannello di navigazione, seleziona Users (Utenti).
3. Nell'elenco degli utenti, seleziona il nome utente. Nella sezione Summary (Riepilogo) viene visualizzato l'ARN dell'utente IAM. L'ARN sarà simile al seguente esempio: arn:aws:iam::123456789012:user/John.

Per trovare l'ARN dell'argomento SNS

1. Apri la console Amazon SNS all'indirizzo https://console.aws.amazon.com/sns/v3/home.
2. Nel pannello di navigazione, scegli Topics (Argomenti).
3. Nell'elenco degli argomenti, gli ARN dell'argomento SNS vengono visualizzati nella colonna ARN. L'ARN è simile a quello riportato di seguito: arn:aws:sns:us-east-1:444455556666:my-sns-topic.

Utilizzo delle notifiche del mittente delegato per l'autorizzazione all'invio di Amazon SES

In qualità di mittente delegato, invii e-mail per conto di un'identità che non è di tua proprietà, ma che sei autorizzato a utilizzare; tuttavia, i messaggi non recapitati e i reclami sono conteggiati nelle tue metriche relative a mancati recapiti e reclami, non in quelle del proprietario dell'identità.

Se la percentuale di mancato recapito o reclamo per il tuo account è troppo elevato, il tuo account è a rischio di essere messo sotto verifica o di avere la sua capacità di inviare email in pausa. Per questo motivo, è importante configurare le notifiche e adottare un processo per monitorarle. È inoltre necessario disporre di un processo per la rimozione dalle tue mailing list degli indirizzi che generano mancati recapiti o reclami.

Pertanto, in qualità di mittente delegato, puoi configurare Amazon SES per inviare notifiche quando si verificano eventi di mancato recapito e reclamo per le e-mail che invii per conto di eventuali identità che non sono di tua proprietà, ma che sei stato autorizzato a utilizzare dal proprietario dell'identità.

Puoi anche configurare la pubblicazione di eventi per pubblicare notifiche di rimbalzi e reclami su Amazon SNS o Firehose.

> **Note**
>
> Se hai configurato Amazon SES per l'invio di notifiche utilizzando Amazon SNS, ti saranno addebitate le tariffe Amazon SNS standard per le notifiche ricevute. Per ulteriori informazioni, consulta la pagina dei prezzi di Amazon SNS.

Creare una notifica di un nuovo mittente delegato

Puoi configurare l'invio di notifiche di delega con set di configurazione utilizzando la pubblicazione di eventi o con identità verificate configurate con i tuoi argomenti SNS.

Di seguito sono riportate le procedure per impostare notifiche di invio di nuovi delegati utilizzando uno dei due metodi:

- Pubblicazione di un evento tramite un set di configurazione
- Notifiche di feedback sugli argomenti SNS di tua proprietà

Per impostare la pubblicazione di eventi tramite un set di configurazione per l'invio dei delegati

1. Accedi alla AWS Management Console e apri la console Amazon SES all'indirizzo https://console.aws.amazon.com/ses/.
2. Seguire le procedure indicate in Crea destinazioni degli eventi.
3. Dopo aver impostato la pubblicazione di eventi nel set di configurazione, specifica il nome del set di configurazione quando invii e-mail come mittente delegato utilizzando l'identità verificata da cui il proprietario dell'identità ti ha autorizzato a inviare. Per informazioni, consulta Invio di e-mail per conto del proprietario di identità.

Per impostare le notifiche di feedback sugli argomenti SNS di tua proprietà per l'invio dei delegati

1. Dopo aver deciso quale dei tuoi argomenti SNS utilizzare per le notifiche di feedback, segui le procedure per trovare l'ARN dell'argomento SNS e copia l'ARN completo e condividilo con il proprietario della tua identità.
2. Chiedi al proprietario dell'identità di configurare i tuoi argomenti SNS per le notifiche di feedback sull'identità condivisa da cui ti ha autorizzato a inviare. Il titolare dell'identità dovrà seguire

le procedure previste per la configurazione di argomenti SNS nelle procedure della policy di autorizzazione.

Invio di e-mail per conto del proprietario di identità per l'autorizzazione all'invio Amazon SES

Come mittente delegato, puoi inviare e-mail nello stesso modo di altri mittenti Amazon SES, a patto che fornisci l'ARN dell'identità che il proprietario di identità ti ha autorizzato a utilizzare. Quando chiami Amazon SES per inviare l'e-mail, Amazon SES verifica se l'identità che hai specificato disponga di una policy che ti autorizza all'invio per suo conto.

Ci sono diversi modi in cui puoi specificare l'ARN dell'identità quando invii un'e-mail. Il metodo che puoi utilizzare dipende se invii l'e-mail utilizzando le operazioni API Amazon SES o l'interfaccia SMTP Amazon SES.

> **Important**
>
> Per inviare correttamente un'e-mail, devi connetterti all'endpoint Amazon SES nella Regione AWS in cui il proprietario di identità ha verificato l'identità.
> Inoltre, gli account AWS del proprietario dell'identità e del mittente delegato devono essere rimossi dalla sandbox prima che gli account possano inviare e-mail a indirizzi non verificati. Per ulteriori informazioni, consultare Richiedi l'accesso alla produzione (uscita dalla sandbox di Amazon SES).

Utilizzo dell'API Amazon SES

Come per qualsiasi mittente di posta elettronica in Amazon SES, se effettui l'accesso ad Amazon SES tramite l'API Amazon SES (o direttamente tramite HTTPS o indirettamente attraverso un SDK AWS), puoi scegliere una tra le tre operazioni di invio di e-mail: `SendEmail`, `SendTemplatedEmail` e `SendRawEmail`. Nella Documentazione di riferimento per le API Amazon Simple Email Service vengono descritti i dettagli di queste API, ma di seguito forniamo una panoramica dei parametri di autorizzazione all'invio.

SendRawEmail

Se desideri utilizzare `SendRawEmail` per poter controllare il formato delle e-mail, puoi specificare l'identità autorizzata delegata in uno di questi due modi:

- Passaggio dei parametri facoltativi all'API **`SendRawEmail`**. I parametri obbligatori sono descritti nella tabella seguente:

Parametro	Descrizione
`SourceArn`	ARN dell'identità associata con la policy di autorizzazione che ti consente di inviare per l'indirizzo e-mail specificato nel parametro `Source` di `SendRawEmail` . **Note** Se specifichi solo `SourceArn` , Amazon SES imposta gli indirizzi "Da" e "Percorso di ritorno" sull'identità specificata in `SourceArn` .
`FromArn`	ARN dell'identità associata con la policy di autorizzazione che ti consente di specificare un particolare indirizzo mittente nell'intestazione dell'e-mail in formato RAW.
`ReturnPathArn`	ARN dell'identità associata con la policy di autorizzazione che ti consente di utilizzare l'indirizzo e-mail specificato nel parametro `ReturnPath` di `SendRawEmail` .

- Inclusione dei campi X-header nell'e-mail. I campi X-header sono intestazioni personalizzate che puoi utilizzare in aggiunta alle intestazioni e-mail standard (ad esempio le intestazioni mittente, reply-to o oggetto). Amazon SES riconosce tre campi X-header che puoi utilizzare per specificare l'invio di parametri di autorizzazione:

Important

Non includere questi campi X-header nella firma DKIM, perché vengono rimossi da Amazon SES prima di inviare l'e-mail.

X-header	Descrizione
X-SES-SOURCE-ARN	Corrisponde a SourceArn .
X-SES-FROM-ARN	Corrisponde a FromArn.
X-SES-RETURN-PATH-ARN	Corrisponde a ReturnPathArn .

Amazon SES rimuove tutti i campi X-header dall'email prima di inviarla. Se includi più istanze di un campo X-header, Amazon SES utilizza solo la prima istanza.

L'esempio seguente mostra un'e-mail che include l'invio di X-header di autorizzazione:

```
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 e SendTemplatedEmail

Se utilizzi l'operazione `SendEmail` o `SendTemplatedEmail`, puoi specificare l'identità autorizzata delegata passando seguenti i parametri facoltativi. Non puoi utilizzare il metodo X-header quando utilizzi l'operazione`SendEmail` o `SendTemplatedEmail`.

Parametro	Descrizione
`SourceArn`	ARN dell'identità associata alla policy di autorizzazione che ti consente di inviare per l'indirizzo e-mail specificato nel parametro `Source` di `SendEmail` o `SendTemplatedEmail` .
`ReturnPathArn`	ARN dell'identità associata con la policy di autorizzazione che ti consente di utilizzare l'indirizzo e-mail specificato nel parametro `ReturnPath` di `SendEmail` o `SendTemplatedEmail` .

L'esempio seguente mostra come inviare un'e-mail che includa gli attributi `SourceArn` e `ReturnPathArn` utilizzando il comando `SendEmail` o `SendTemplatedEmail` e l'SDK per 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'])
```

Utilizzo dell'interfaccia SMTP Amazon SES

Quando utilizzi l'interfaccia SMTP Amazon SES per l'invio dei delegati, devi includere le intestazioni `X-SES-SOURCE-ARN`, `X-SES-FROM-ARN` e `X-SES-RETURN-PATH-ARN` nel messaggio. Passa queste intestazioni dopo l'esecuzione del comando `DATA` nella conversazione SMTP.

Invio di e-mail di prova in Amazon SES con il simulatore

Consigliamo di utilizzare la console Amazon SES per inviare un'e-mail di prova con Amazon SES. Poiché la console richiede l'immissione manuale di informazioni, in genere devi usarla solo per inviare e-mail di prova. Quando inizi a usare Amazon SES, molto probabilmente invierai le tue e-mail tramite l'interfaccia SMTP o l'API di Amazon SES. Tuttavia, la console è utile per monitorare l'attività di invio.

I seguenti argomenti illustrano come utilizzare il simulatore di mailbox sia dalla console che manualmente inviando e-mail:

- Utilizzo del simulatore di mailbox dalla console
- Utilizzo manuale del simulatore di mailbox

Utilizzo del simulatore di mailbox dalla console

> **Important**
>
> - In questo tutorial ti invierai un'e-mail dalla console, in modo da controllare se la ricevi. Per ulteriori sperimentazioni o test di carico, consulta Utilizzo manuale del simulatore di mailbox.
> - Oltre a non essere conteggiate ai fini della quota di invio o delle percentuali di mancati recapiti (bounce) e reclami, le e-mail inviate al simulatore di mailbox non influenzano i parametri di Virtual Deliverability Manager.

Prima di seguire questi passaggi, completa le attività descritte in Impostazione di Amazon Simple Email Service.

Invio di un messaggio e-mail di prova dalla console Amazon SES

1. Accedi alla AWS Management Console e apri la console Amazon SES all'indirizzo https://console.aws.amazon.com/ses/.
2. Nel pannello di navigazione, in Configuration (Configurazione), scegli Verified identities (Identità verificate).
3. Dalla tabella Identities (Identità), seleziona un'identità e-mail verificata facendo clic direttamente sul nome dell'identità anziché selezionandone la casella di controllo. Se non disponi di un'identità e-mail verificata, consulta Creazione di un'identità dell'indirizzo e-mail.
4. Nella pagina dei dettagli dell'identità e-mail selezionata, scegli Send test email (Invia e-mail di prova).
5. Per Message details (Dettagli messaggio), scegli Email Format (Formato e-mail). Sono disponibili le due opzioni seguenti:

   - Formatted (Formattata): questa è l'opzione più semplice. Scegli questa opzione se vuoi semplicemente digitare il testo del messaggio nella casella di testo Body (Corpo). Quando invii l'e-mail, Amazon SES applica al testo il formato di e-mail automaticamente.
   - Raw: scegli questa opzione se vuoi inviare un messaggio più complesso, ad esempio un messaggio che include contenuto HTML o un allegato. A causa di questa flessibilità, devi formattare personalmente il messaggio, come descritto in Invio di e-mail non elaborate

utilizzando l'API Amazon SES v2, quindi incollare l'intero messaggio formattato, incluse le intestazioni, nella casella di testo Body (Corpo). Puoi usare l'esempio seguente, che include contenuto HTML, per inviare un'e-mail di prova usando il formato e-mail Raw. Copia e incolla questo messaggio completo nella casella di testo Body (Corpo). Assicurati che non vi sia una riga vuota tra l'intestazione `MIME-Version` e l'intestazione `Content-Type`; in caso contrario, l'e-mail avrebbe un formato di testo normale invece che 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. Scegli il tipo di scenario di e-mail simulato che desideri testare espandendo la casella dell'elenco Scenario.

   - Se scegli Custom (Personalizzato) e ti trovi ancora nella sandbox Amazon SES, assicurati che l'indirizzo specificato nel campo Custom recipient (Destinatario personalizzato) sia un indirizzo e-mail verificato. Per ulteriori informazioni, consulta Creazione di un'identità dell'indirizzo e-mail.

7. Compila i campi rimanenti come desiderato.
8. Scegli Send a Test Email (Invia e-mail di prova).
9. Accedi al client e-mail dell'indirizzo al quale hai inviato l'e-mail. Troverai il messaggio inviato.

Utilizzo manuale del simulatore di mailbox

Amazon SES include un simulatore di mailbox che puoi utilizzare per testare il modo in cui la tua applicazione gestisce diversi scenari di invio di e-mail. Il simulatore di mailbox è utile, ad esempio, se hai bisogno di testare un'applicazione per l'invio di e-mail senza la creazione di indirizzi e-mail fittizi, oppure se devi individuare la velocità effettiva massima del tuo sistema senza compromettere la quota di invio giornaliera.

Considerazioni importanti

Quando utilizzi il simulatore di mailbox Amazon SES considera le seguenti caratteristiche e limitazioni:

- Puoi utilizzare il simulatore di mailbox anche se il tuo account è nella sandbox Amazon SES.
- Le e-mail inviate al simulatore di mailbox sono limitate dalla frequenza massima in uscita del tuo account, ma non influenzano le quote di invio giornaliere. Ad esempio, se il tuo account è autorizzato a inviare 10.000 messaggi per un periodo di 24 ore e invii 100 messaggi al simulatore di mailbox, potrai comunque inviare fino a 10.000 messaggi a normali destinatari senza raggiungere la quota di invio.
- Le e-mail inviate al simulatore di mailbox non impattano sull'efficienza del recapito delle tue e-mail o sui parametri di reputazione. Ad esempio, se invii un numero elevato di messaggi all'indirizzo del simulatore di e-mail che causano il mancato recapito, non mostrerà alcun messaggio indicante che il tuo tasso di mancato recapito è troppo elevato nella pagina della console dei parametri di reputazione.
- Ai fini della fatturazione, le e-mail inviate al simulatore di mailbox Amazon SES sono considerare esattamente come qualsiasi altro messaggio e-mail inviato utilizzando Amazon SES. In altre parole, ti verranno fatturati per lo stesso importo sia i messaggi inviati al simulatore di mailbox sia quelli inviati ai normali destinatari.
- Il simulatore di mailbox supporta l'etichettatura, che consente di inviare e-mail allo stesso indirizzo del simulatore di mailbox in vari modi oppure di testare il modo in cui la tua applicazione gestisce il VERP (Variable Envelope Return Path). Ad esempio, puoi inviare un'e-mail a bounce+label1@simulator.amazonses.com e bounce+label2@simulator.amazonses.com per verificare se la tua applicazione è in grado di abbinare un messaggio di mancato recapito con l'indirizzo e-mail che ha causato il mancato recapito.
- Se utilizzi il simulatore di mailbox per simulare più mancati recapiti dalla stessa richiesta di invio, Amazon SES combina le risposte di mancato recapito in una singola risposta.

Utilizzo del simulatore di mailbox

Per utilizzare il simulatore di e-mail, individua lo scenario nella tabella riportata di seguito, quindi invia un'e-mail all'indirizzo e-mail corrispondente.

> **Note**
>
> Quando invii un'e-mail all'indirizzo del simulatore di mailbox, devi inviarla tramite Amazon SES, utilizzando l'AWS CLI, un SDK AWS, la console Amazon SES, l'interfaccia SMTP Amazon SES o l'API Amazon SES. Il simulatore di mailbox non risponde alle e-mail ricevute da fonti esterne.

Scenario simulato	Indirizzo e-mail
Consegna eseguita correttamente: il provider di posta elettronica del destinatario accetta la tua e-mail. Se hai impostato le notifiche di consegna come descritto in Impostazione delle notifiche degli eventi per Amazon SES, Amazon SES invia una notifica di consegna tramite Amazon Simple Notification Service (Amazon SNS).	success@simulator.amazonses.com
Mancato recapito: l'ISP del destinatario rifiuta la tua e-mail con un codice di risposta SMTP 550 5.1.1 ("Utente sconosciuto"). Amazon SES genera una notifica di mancato recapito e, in base alle impostazioni del tuo account, te la invia tramite e-mail o invia una notifica a un argomento Amazon SNS. L'indirizzo e-mail del simulatore di mailbox non è collocato nella lista di soppressione Amazon SES, come accade normalmente in caso di mancato recapito permanente. La risposta di mancato recapito ricevuta dal simulatore di mailbox è conforme allo standard RFC 3464. Per informazioni su come ricevere feedback sul mancato recapito, consulta Impostazione delle notifiche degli eventi per Amazon SES.	bounce@simulator.amazonses.com

Scenario simulato	Indirizzo e-mail
Risposte automatiche: il provider di posta elettronica del destinatario accetta la tua e-mail e la consegna alla casella di posta in arrivo del destinatario. Il provider di posta elettronica invia una risposta automatica, ad esempio un messaggio di "fuori sede", all'indirizzo indicato nell'intestazione del percorso di ritorno dell'e-mail, oppure all'indirizzo della busta del mittente ("MAIL FROM") qualora l'intestazione del percorso di ritorno non sia presente. La risposta automatica che ricevi dal simulatore di mailbox è conforme allo standard RFC 3834.	ooto@simulator.amazonses.com
Reclamo: il provider di posta elettronica del destinatario accetta la tua e-mail e la consegna alla casella di posta in arrivo del destinatario. Il destinatario stabilisce che il messaggio non è stato richiesto e clicca su "Contrassegna come spam" nel suo client di posta elettroni ca. Amazon SES ti inoltra quindi la notifica di reclamo tramite e-mail o utilizzando una notifica Amazon SNS, in base alla modalità di impostazione dell'account. La risposta di reclamo ricevuta dal simulatore di mailbox è conforme allo standard RFC 5965. Per informazioni su come ricevere feedback sul reclamo, consulta Impostazione delle notifiche degli eventi per Amazon SES.	complaint@simulator.amazonses.com
Indirizzo del destinatario presente sulla lista di eliminazione: Amazon SES genera un mancato recapito permanente come se l'indiriz zo del destinatario fosse presente sulla lista di eliminazione.	suppressionlist@simulator.amazonses.com

Test degli eventi di rifiuto

Per ogni messaggio inviato tramite Amazon SES viene eseguita la scansione per la ricerca di virus. Se invii un messaggio che contiene un virus, Amazon SES accetta il messaggio, rileva il virus e respinge l'intero messaggio. Quando Amazon SES rifiuta un messaggio, interrompe l'elaborazione e non tenta di inviarlo al server di posta elettronica del destinatario. Ciò genera un evento di rifiuto.

Il simulatore di mailbox Amazon SES non include un indirizzo per il test degli eventi di rifiuto. Tuttavia, puoi testare gli eventi di rifiuto utilizzando un file di test EICAR (European Institute for Computer Antivirus Research). Questo file rappresenta un metodo standard del settore per il test di software antivirus in modo sicuro. Per creare un file di test EICAR, incolla il testo seguente in un file:

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

Salva il file come `sample.txt`, allegalo a un'e-mail, quindi invia il messaggio e-mail a un indirizzo verificato. Se non vi sono altri problemi con l'e-mail, Amazon SES accetta il messaggio, ma poi lo rifiuta come se l'istanza contenesse effettivamente un virus.

> **Note**
>
> Le e-mail rifiutate, incluse quelle inviate utilizzando la procedura sopra indicata, sono conteggiate ai fini della quota di invio giornaliera. Viene fatturato ogni messaggio inviato, inclusi i messaggi rifiutati.

Per ulteriori informazioni sui file di test EICAR , consulta la relativa pagina su Wikipedia.

Utilizzo dei set di configurazione in Amazon SES

I set di configurazione sono gruppi di regole che è possibile applicare alle identità verificate. Un'identità verificata è un dominio o un indirizzo e-mail che si utilizza per inviare messaggi e-mail mediante Amazon SES. Quando applichi un set di configurazione a un'e-mail, tutte le regole nel set di configurazione vengono applicate all'e-mail.

Puoi usare i set di configurazione per applicare i tipi di regole seguenti all'invio di e-mail e puoi contenere uno di questi tipi, entrambi i tipi o nessuno:

- Destinazioni degli eventi: ti consentono di pubblicare le metriche di invio di e-mail, tra cui il numero di invii, consegne, aperture, clic, rimbalzi e reclami su altri AWS prodotti per ogni e-mail inviata. Ad esempio, puoi inviare i parametri delle tue e-mail a una destinazione Amazon Data Firehose e quindi analizzarli utilizzando Amazon Managed Service per Apache Flink. In alternativa, puoi inviare le informazioni relative a mancati recapiti e reclami ad Amazon SNS e ricevere immediatamente notifiche quando tali eventi si verificano.
- Gestione di pool di IP: in caso di noleggio di indirizzi IP dedicati da usare con Amazon SES, puoi creare gruppi di questi indirizzi, denominati pool di IP dedicati, da usare per l'invio di tipi specifici di e-mail. Ad esempio, puoi associare questi pool IP dedicati ai set di configurazione e utilizzarne uno per l'invio di comunicazioni di marketing e un altro per l'invio di e-mail transazionali. La tua reputazione di mittente per le e-mail transazionali è quindi isolata da quella delle e-mail di marketing.

Puoi associare un set di configurazione a un'identità verificata nei modi seguenti:

- Includi un riferimento alla configurazione impostata nelle intestazioni dell'e-mail. Per ulteriori informazioni su come specificare i set di configurazione nelle e-mail, consulta Specifica di un set di configurazione per l'invio di e-mail.
- Specifica un set di configurazione esistente da utilizzare come set di configurazione predefinito dell'identità al momento della creazione dell'identità o successivamente durante la modifica di un'identità verificata. Per informazioni, consulta Informazioni sui set di configurazione predefiniti.

Indice

- Specifica di un set di configurazione per l'invio di e-mail
- Visualizzazione ed esportazione dei parametri di reputazione

Creazione di set di configurazione in SES

Per creare un nuovo set di configurazione, puoi utilizzare la console SES, l'operazione `CreateConfigurationSet` nell'API Amazon SES v2, o il comando `aws sesv2 create-configuration-set` nella CLI v2 di Amazon SES. Questa sezione mostra come creare set di configurazione utilizzando la console SES e la CLI v2 di Amazon SES.

Creazione di un set di configurazione (console)

Per creare un set di configurazione tramite la console SES, attieniti alla seguente procedura:

1. Accedi AWS Management Console e apri la console Amazon SES all'indirizzo https://console.aws.amazon.com/ses/.
2. Nel pannello di navigazione, in Configuration (Configurazione), scegli Configuration sets (Set di configurazione).
3. Seleziona Create asset (Crea asset).
4. Immetti i seguenti dati nella sezione General details (Dettagli generali):

   - Configuration set name (nome del set di configurazione): digita un nome per il set di configurazione. Il nome può contenere fino a 64 caratteri alfanumerici, inclusi lettere, numeri, trattini (-) e trattini bassi (_).
   - Sending IP pool (Invio di pool IP): quando si inviano messaggi di posta elettronica utilizzando questo set di configurazione, i messaggi vengono inviati dagli indirizzi IP dedicati nel pool assegnato. Seleziona un pool di IP dall'elenco.

     > **Note**
     >
     > L'impostazione di default (ses-default-dedicated-pool) contiene indirizzi IP dedicati che non sono stati assegnati a nessun altro pool. Per ulteriori informazioni sulla gestione dei pool di IP, consulta Assegnazione di pool di IP.

   - Opzioni di monitoraggio: seleziona la casella di controllo Utilizza un dominio di reindirizzamento personalizzato per utilizzare un dominio di reindirizzamento personalizzato

per gestire il monitoraggio di apertura e di clic per questo set di configurazione, invece di utilizzare uno dei domini SES.

- Custom redirect domain (Dominio di reindirizzamento personalizzato): con un dominio di reindirizzamento personalizzato, è possibile immettere un sottodominio personalizzato nella casella (facoltativo) oppure selezionare un dominio verificato dall'elenco.

> **Note**
>
> I domini di reindirizzamento personalizzati possono essere specificati come segue:
>
> - I domini di reindirizzamento devono essere impostati prima di scegliere questa opzione. Per istruzioni su come selezionare un dominio personalizzato per gestire il monitoraggio di apertura e clic, consulta Configurazione di domini personalizzati per gestire il monitoraggio di aperture e clic.
> - Quindi, per scegliere di utilizzare un dominio di reindirizzamento personalizzato, è necessario indicarlo durante la creazione del set di configurazione o in un secondo momento modificando le opzioni di monitoraggio per il set di configurazione.

- Advanced delivery options (Opzioni di consegna avanzate): scegli la freccia a sinistra per espandere la sezione delle opzioni di consegna avanzate.
  - Transport Layer Security (TLS): per richiedere a SES di stabilire una connessione sicura con il server di posta ricevente e inviare e-mail utilizzando il protocollo TLS, seleziona la casella di controllo Obbligatorio.

> **Note**
>
> SES supporta TLS 1.2 e suggerisce TLS 1.3. Per ulteriori informazioni, consulta Sicurezza dell'infrastruttura in SES.

5. Immetti i seguenti dati nella sezione Reputation options (Opzioni di reputazione):

- Metriche sulla reputazione: utilizzate per tenere traccia delle metriche relative a rimbalzi e reclami CloudWatch per le e-mail inviate utilizzando questo set di configurazione. (Si applicano costi aggiuntivi, vedi Prezzo per metrica). CloudWatch
  - Enabled (Abilitati): selezionare questa casella di controllo per abilitare i parametri di reputazione per il set di configurazione.

6.

La sezione Suppression list options (Opzioni elenco di eliminazione) fornisce un set di decisioni per definire l'eliminazione personalizzata a partire dall'opzione di utilizzare questo set di configurazione per sovrascrivere l'eliminazione a livello di account. La mappa logica di eliminazione a livello di set di configurazione ti aiuterà a comprendere gli effetti delle combinazioni di sovrascrittura. Queste selezioni su più livelli di sovrascrittura possono essere combinate per implementare tre diversi livelli di eliminazione:

a. Use account-level suppression (Usa eliminazione a livello di account): non sovrascrivere l'eliminazione a livello di account e non implementare alcuna eliminazione a livello di set di configurazione. Fondamentalmente, qualsiasi e-mail inviata utilizzando questo set di configurazione utilizzerà solo l'eliminazione a livello di account. Per farlo:

   - In Suppression list settings (Impostazioni elenco di eliminazione), deseleziona la casella Override account level settings (Sovrascrivi impostazioni a livello di account).

b. Do not use any suppression (Non usare alcuna eliminazione): sovrascrivi l'eliminazione a livello di account senza abilitare l'eliminazione a livello di set di configurazione. Questo significa che qualsiasi e-mail inviata utilizzando questo set di configurazione non utilizzerà alcuna eliminazione a livello di account. In altre parole, tutta l'eliminazione viene annullata. Per farlo:

   i. In Suppression list settings (Impostazioni elenco di eliminazione), controlla la casella Override account level settings (Sovrascrivi impostazioni a livello di account).

   ii. In Suppression list (Elenco di eliminazione), deseleziona la casella Enabled (Abilitato).

c. Use configuration set-level suppression (Usa eliminazione a livello di set di configurazione): sostituisci l'eliminazione a livello di account con impostazioni personalizzate dell'elenco di eliminazione definite in questo set di configurazione. Questo significa che qualsiasi e-mail inviata utilizzando questo set di configurazione utilizzerà solo le proprie impostazioni di eliminazione e ignorerà le impostazioni di eliminazione a livello di account. Per farlo:

   i. In Suppression list settings (Impostazioni elenco di eliminazione), controlla la casella Override account level settings (Sovrascrivi impostazioni a livello di account).

   ii. In Suppression list (Elenco di eliminazione), seleziona Enabled (Abilitato).

   iii. In Specify the reason(s)… (Specificare i motivi…), seleziona uno dei motivi dell'eliminazione da utilizzare per questo set di configurazione.

7.

La sezione Virtual Deliverability Manager options (Opzioni di Virtual Deliverability Manager) consente di definire impostazioni personalizzate relative al modo in cui questo set di configurazione utilizzerà il monitoraggio del coinvolgimento e la consegna condivisa ottimizzata, sovrascrivendo quelle definite nelle impostazioni di Virtual Deliverability Manager a livello di account:

a. Per disabilitare sia il monitoraggio del coinvolgimento sia la consegna condivisa ottimizzata per questo set di configurazione:

   i. Seleziona la casella Override account level settings (Sovrascrivi le impostazioni a livello di account).

   ii. Assicurati che l'opzione Enabled (Abilitato) sia deselezionata sia per Engagement tracking (Monitoraggio del coinvolgimento) sia per Optimized shared delivery (Consegna condivisa ottimizzata), quindi scegli Save changes (Salva modifiche).

b. Per abilitare o disabilitare il monitoraggio del coinvolgimento o la consegna condivisa ottimizzata oppure entrambi per questo set di configurazione:

   i. Seleziona la casella Override account level settings (Sovrascrivi le impostazioni a livello di account).

   ii. Seleziona o deseleziona Enabled (Abilitato) per una o entrambe le opzioni Engagement tracking (Monitoraggio del coinvolgimento) e Optimized shared delivery (Consegna condivisa ottimizzata), quindi scegli Save changes (Salva modifiche).

c. Per ripristinare le impostazioni a livello di account di Virtual Deliverability Manager per il monitoraggio del coinvolgimento e la consegna condivisa ottimizzata per questo set di configurazione:

   • Deseleziona la casella Override account level settings (Sovrascrivi le impostazioni a livello di account), quindi scegli Save changes (Salva modifiche).

8. È possibile aggiungere facoltativamente uno o più tag nella sezione Tags (Tag). Ripeti i seguenti passaggi per ogni tag che desideri aggiungere al set di configurazione.

   a. Scegli Add new tag (Aggiungi nuovo tag).

   b. Inserisci il valore per Key (Chiave) del tag.

   c. Inserisci il valore per Value (Valore) del tag (facoltativo).

Per rimuovere un tag immesso, scegli Remove (Rimuovi) per quel tag. È possibile aggiungere un massimo di 50 tag.

9. Scegli Create set (Crea set) per creare il set di configurazione.

Ora che hai creato il set di configurazione, hai la possibilità di definire le destinazioni degli eventi per il set di configurazione che consente la pubblicazione di eventi attivata sui tipi di eventi specificati per la destinazione dell'evento. Un set di configurazione può avere più destinazioni eventi con più tipi di eventi definiti. Per informazioni, consulta Creazione delle destinazioni degli eventi Amazon SES.

Creazione di un set di configurazione (AWS CLI)

È possibile creare un set di configurazione utilizzando un file JSON come input per il comando `aws sesv2 create-configuration-set` nell' AWS CLI.

1. Creazione di un file JSON di input nella CLI

   Utilizza lo strumento di modifica dei file preferito per creare un file JSON con le seguenti chiavi, oltre a valori validi per l'ambiente in uso, oppure utilizza il comando `aws sesv2 create-configuration-set` dell'API SES v2 con l'opzione `--generate-cli-skeleton` senza alcun valore specificato per stampare una struttura JSON di esempio su output standard.

   In questo esempio viene utilizzato un file denominato `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**
>
> - È necessario includere l'annotazione `file://` all'inizio del percorso del file JSON.
> - Il percorso del file JSON deve seguire la convenzione appropriata per il sistema operativo di base in cui si esegue il comando. Ad esempio, Windows utilizza la barra rovesciata (\) per fare riferimento al percorso della directory e Linux usa la barra (/).

2. Esegui il comando seguente utilizzando il file creato come input.

```
aws sesv2 create-configuration-set --cli-input-json file://create-configuration-set.json
```

> **Note**
>
> Per esaminare il AWS CLI riferimento a questo comando, consulta create-configuration-set.

Gestione dei set di configurazione in Amazon SES

Dopo aver creato un set di configurazione, puoi gestirlo con le opzioni di visualizzazione, modifica ed eliminazione utilizzando la console SES, l'API v2 Amazon SES e l'interfaccia CLI v2 di Amazon SES. I set di configurazione possono anche essere assegnati a un'identità verificata come set di configurazione predefinito che viene applicato ogni volta che un'e-mail viene inviata dall'identità.

Argomenti in questa sezione:

- Visualizzazione, modifica ed eliminazione del set di configurazione (console)

- Elenco dei set di configurazione (AWS CLI)
- Ottenimento dei dettagli del set di configurazione (AWS CLI)
- Eliminazione di set di configurazione (AWS CLI)
- Interruzione dell'invio di e-mail da un set di configurazione (AWS CLI)
- Informazioni sui set di configurazione predefiniti
- Creazione delle destinazioni degli eventi Amazon SES
- Assegnazione di pool di IP in Amazon SES
- Configurazione di domini personalizzati per gestire il monitoraggio di aperture e clic

Visualizzazione, modifica ed eliminazione del set di configurazione (console)

Accedi alla pagina dei dettagli di un set di configurazione esistente.

1. Accedi AWS Management Console e apri la console Amazon SES all'indirizzo https://console.aws.amazon.com/ses/.
2. Nel pannello di navigazione, in Configuration (Configurazione), scegli Configuration sets (Set di configurazione).
3. Per visualizzare altri dettagli relativi a una configurazione, scegli il nome dall'elenco dei set di configurazione. In questo modo si accede alla pagina dei dettagli.

La pagina dei dettagli Configuration sets (Set di configurazione) comprende due schede per i dettagli del set di configurazione con pannelli in ogni scheda in cui è possibile visualizzare, modificare o eliminare come segue:

- Scheda Overview (Panoramica)
  - General details (Dettagli generali): questo pannello mostra i dettagli generali per il set di configurazione:
    - Sending status (Stato di invio) (se è attualmente abilitato)
    - Configuration set name (Nome del set di configurazione)
    - Sending IP pool (Pool di IP di invio)
    - Transport Layer Security (TLS)
    - Custom redirect domain (Dominio di reindirizzamento personalizzato)

- Reputation options (Opzioni di reputazione): questo pannello mostra i dettagli relativi alla tua reputazione di invio:
  - Reputation metrics (Parametri di reputazione) (indica se stai monitorando i parametri)
  - Last fresh start (Ultimo nuovo inizio) (la data e l'ora in cui i parametri di reputazione del set di configurazione sono stati reimpostati per l'ultima volta)
- Suppression list options (Opzioni dell'elenco di soppressione): questo pannello mostra se stai sovrascrivendo l'elenco di soppressione a livello di account con il set di configurazione e, in tal caso, quali sono i relativi dettagli:
  - Suppression list settings (Impostazioni dell'elenco di soppressione): indica la sovrascrittura delle impostazioni a livello di account; se non è così, questo è l'unico elemento visualizzato nel pannello
  - Suppression list (Elenco delle soppressioni): indica in che modo vengono sovrascritte le impostazioni a livello di account, con l'elenco di soppressione abilitato o disabilitato
  - Suppression reasons (Motivi della soppressione): indica se i mancati recapiti e/o i reclami sono il motivo dell'aggiunta all'elenco di soppressione degli indirizzi e-mail dei destinatari
- Virtual Deliverability Manager options (Opzioni di Virtual Deliverability Manager): questo pannello mostra se le impostazioni dell'account Virtual Deliverability Manager per il monitoraggio del coinvolgimento e la consegna condivisa ottimizzata vengono sovrascritte con il set di configurazione e, in caso affermativo, quali sono i relativi dettagli:
  - Engagement tracking (Monitoraggio del coinvolgimento): indica se il monitoraggio del coinvolgimento è abilitato o disabilitato
  - Optimized shared delivery (Consegna condivisa ottimizzata): indica se la consegna condivisa ottimizzata è abilitata o disabilitata
- Tags (Tag): questo pannello mostra tutti i tag allegati al set di configurazione.
  - Key (Chiave)
  - Value (Valore)

Da questi pannelli puoi eseguire le seguenti operazioni:

- Scegli il pulsante Edit (Modifica) oppure, nel caso del pannello Tags (Tag), il pulsante Manage tags (Gestisci tag) per modificare i rispettivi dettagli di ciascun pannello.
- Per ulteriori informazioni sui campi, consulta la sezione correlata nei passaggi Creazione di un set di configurazione (console).

> **Tip**
>
> Ricordati di selezionare Save changes (Salva le modifiche) quando hai finito di modificare. Scegli Cancel (Annulla) per tornare alla pagina dei dettagli del set di configurazione senza salvare.

- Scheda Event destinations (Destinazioni degli eventi)
  - All destinations (***`count of event destinations`***) (Tutte le destinazioni (conteggio delle destinazioni dell'evento)): questo pannello elenca tutte le destinazioni degli eventi immesse per il set di configurazione. Per ciascuna destinazione, puoi consultare:
    - Name (Nome)
    - Destination (Destinazione)
    - Event types (Tipi di evento)
    - Event publishing (Pubblicazione degli eventi)

  Da questo pannello puoi eseguire le seguenti operazioni:

  - Aggiungi una nuova destinazione degli eventi scegliendo il pulsante Add destination (Aggiungi destinazione). Per ulteriori informazioni sulla configurazione delle destinazioni di eventi, consulta Creazione di una destinazione degli eventi.
  - Modifica una destinazione degli eventi esistente selezionandone il nome, che aprirà la schermata di modifica.
  - Elimina una destinazione degli eventi esistente selezionando la casella di controllo accanto al suo nome e scegliendo il pulsante Delete (Elimina).

Nella parte superiore della pagina dei dettagli di ogni set di configurazione, visibili dalla scheda Overview (Panoramica) o Events destination (Destinazione eventi), si trovano le seguenti opzioni:

- Delete (Elimina): questo pulsante eliminerà il set di configurazione.
- Disable sending (Disabilita invio): questo pulsante interromperà l'invio di messaggi di posta elettronica dal set di configurazione.

Elenco dei set di configurazione (AWS CLI)

Puoi utilizzare il list-configuration-sets comando in AWS CLI per generare un elenco di tutti i set di configurazione associati al tuo account nella regione corrente, come segue:

```
aws sesv2 list-configuration-sets
```

Ottenimento dei dettagli del set di configurazione (AWS CLI)

È possibile utilizzare il get-configuration-set comando in per AWS CLI ottenere i dettagli per un set di configurazione specifico, come segue:

```
aws sesv2 get-configuration-set --configuration-set-name name
```

Eliminazione di set di configurazione (AWS CLI)

È possibile utilizzare il delete-configuration-set comando in AWS CLI per eliminare un set di configurazione specifico, nel modo seguente:

```
aws sesv2 delete-configuration-set --configuration-set-name name
```

Interruzione dell'invio di e-mail da un set di configurazione (AWS CLI)

È possibile utilizzare il put-configuration-set-sending-options comando in AWS CLI per interrompere l'invio di e-mail da un set di configurazione specifico, come segue:

```
aws sesv2 put-configuration-set-sending-options --configuration-set-name name --no-
sending-enabled
```

Per riattivare nuovamente l'invio, esegui lo stesso comando con il l'opzione `--sending-enabled`, come segue:

```
aws sesv2 put-configuration-set-sending-options --configuration-set-name name --
sending-enabled
```

Informazioni sui set di configurazione predefiniti

Il concetto di assegnazione di un set di configurazione come set predefinito affinché sia utilizzato da un'identità verificata è spiegato in questa sezione per aiutare a comprendere i vantaggi e il caso d'uso.

Un set di configurazione predefinito applica automaticamente le sue regole a tutti i messaggi inviati dall'identità e-mail associata a tale set di configurazione. Puoi applicare set di configurazione predefiniti sia all'indirizzo e-mail che alle identità di dominio durante la creazione dell'identità o in seguito, come funzione di modifica di un'identità esistente.

Considerazioni sul set di configurazione predefinito

- È necessario creare il set di configurazione prima di associarlo a un'identità.
- I set di configurazione predefiniti verranno applicati solo se l'identità è verificata.
- Un'identità e-mail può essere associata a un solo set di configurazione alla volta. Tuttavia, puoi applicare lo stesso set di configurazione a più identità.
- Un set di configurazione predefinito a livello di indirizzo e-mail sovrascrive un set di configurazione predefinito a livello di dominio. Ad esempio, un set di configurazione predefinito associato a joe@example.com sovrascrive il set di configurazione per il dominio di example.com.
- Un set di configurazione predefinito a livello di dominio si applica a tutti gli indirizzi e-mail per quel dominio (a meno che non verifichi indirizzi specifici per il dominio).
- Se elimini un set di configurazione designato come set di configurazione predefinito per un'identità e quindi tenti di inviare e-mail tramite tale identità, la chiamata ad Amazon SES non riesce con un errore di "richiesta errata".
- Un set di configurazione predefinito non può essere assegnato a un'identità verificata utilizzata da unmittente delegato.
- Come specificare un set di configurazione esistente da utilizzare come set di configurazione predefinito dell'identità è in realtà una funzione delle identità verificate, pertanto le istruzioni vengono fornite nei flussi di lavoro delle identità:
  - Specify a default configuration set during identity creation (Specificare un set di configurazione predefinito durante la creazione dell'identità): segui le istruzioni riportate nel passaggio 6 opzionale Domain identity default configuration set (Set di configurazione predefinito dell'identità di dominio) o Email identity default configuration set (Set di configurazione predefinito dell'identità e-mail) nel capitolo Creazione e verifica delle identità in Amazon SES.

- Specify a default configuration set for an existing identity (Specificare un set di configurazione predefinito per un'identità esistente): segui la procedura riportata in Modifica di un'identità tramite la console insieme a questi dettagli per il passaggio 5:
  a. Scegli la scheda Configuration set (Set di configurazione).
  b. Scegli Edit (Modifica) nel container Default configuration set (Set di configurazione predefinito).
  c. Seleziona la casella dell'elenco e scegli un set di configurazione esistente da utilizzare come predefinito.
  d. Continua con i passaggi rimanenti in Modifica di un'identità tramite la console.

> **Note**
>
> Se il set di configurazione assegnato come predefinito ha le metriche di reputazione abilitate, verranno addebitati costi aggiuntivi per qualsiasi posta inviata utilizzando il set di configurazione predefinito, vedi Prezzo per metrica per. CloudWatch

Creazione delle destinazioni degli eventi Amazon SES

Le destinazioni degli eventi consentono di pubblicare le seguenti azioni di tracciamento delle e-mail in uscita su altri servizi per il monitoraggio: AWS

- Invii
- Errori di rendering
- Rifiuti
- Consegne
- Mancati recapiti permanenti
- Reclami
- Ritardi di consegna
- Sottoscrizioni
- Aperture
- Clic

Per ulteriori informazioni su come impostare la pubblicazione di eventi, consulta the section called “Monitoraggio dell'invio di e-mail utilizzando la pubblicazione di eventi”.

Creazione di una destinazione degli eventi

Dopo aver creato un set di configurazione, è possibile creare destinazioni degli eventi per il set di configurazione che consente la pubblicazione di eventi attivata sui tipi di eventi specificati per la destinazione dell'evento. Un set di configurazione può avere più destinazioni degli eventi con più tipi di eventi definiti.

Se non hai ancora creato un set di configurazione, consulta the section called “Creazione di set di configurazione”.

I passaggi seguenti mostrano come creare o aggiungere una destinazione di eventi a un set di configurazione.

Per creare o aggiungere una destinazione degli eventi utilizzando la console SES:

1. Accedi AWS Management Console e apri la console Amazon SES all'indirizzo https://console.aws.amazon.com/ses/.
2. Nel pannello di navigazione, in Configuration (Configurazione), scegli Configuration sets (Set di configurazione).
3. Scegli il nome di un set di configurazione dalla colonna Nome per accedere ai suoi dettagli.
4. Seleziona la scheda Destinazioni degli eventi.
5. Scegli Add destination (Aggiungi destinazione).
6. Selezione dei tipi di evento

   Gli eventi di invio e-mail sono parametri relativi alla tua attività di invio che puoi misurare utilizzando Amazon SES. In questo passaggio, puoi selezionare i tipi di e-mail che inviano eventi che desideri pubblicare da Amazon SES nella destinazione dell'evento.

   Per ulteriori informazioni sui tipi di policy, consulta Monitoraggio delle attività di invio di Amazon SES.

   a. Scegli Event types (Tipi di eventi) per la pubblicazione

      - Sending and delivery (Invio e consegna): per scegliere i tipi di eventi da pubblicare, seleziona le rispettive caselle di controllo o scegli Select all (Seleziona tutto) per pubblicare tutti i tipi di evento.

Event types (Tipi di evento)

- Sends (Invii): la richiesta di invio è stata completata e Amazon SES tenterà la consegna del messaggio al server di posta del destinatario.
- Rendering failures (Fallimenti di rendering): l'e-mail non è stata inviata a causa di un fallimento di rendering del modello. Questo tipo di evento può verificarsi se i dati del modello mancano o se non vi è corrispondenza tra i parametri e i dati del modello. Questo tipo di evento si verifica solo quando invii un'e-mail basata su modello utilizzando le operazioni API `SendTemplatedEmail` o `SendBulkTemplatedEmail`.
- Rejects (Rifiuti): Amazon SES ha accettato l'e-mail, ma ha stabilito che conteneva un virus e non ha tentato di consegnarla al server di posta del destinatario.
- Deliveries (Consegne): Amazon SES ha consegnato correttamente l'e-mail al server e-mail del destinatario.
- Hard bounces (Mancati recapiti permanenti): il server e-mail del destinatario ha rifiutato l'e-mail in modo permanente. (I casi di soft bounce (e-mail non recapitata) sono previsti solo se Amazon SES non riesce a inviare il messaggio e-mail dopo avere ritentato per un determinato periodo di tempo).
- Complaints (Reclami): l'e-mail è stata recapitata correttamente al server di posta del destinatario, ma il destinatario l'ha contrassegnata come spam.
- Delivery delays (Ritardi di consegna): impossibile recapitare l'e-mail al server e-mail del destinatario perché si è verificato un problema temporaneo. I ritardi di consegna possono verificarsi, ad esempio quando la casella di posta in arrivo del destinatario è piena o quando nel server di ricezione della posta elettronica si verifica un problema transitorio. Questo tipo di evento non è supportato da Amazon Pinpoint.
- Subscriptions (Sottoscrizioni): l'e-mail è stata recapitata correttamente, ma il destinatario ha aggiornato le preferenze di sottoscrizione facendo clic su `List-Unsubscribe` nell'intestazione dell'email o sul collegamento `Unsubscribe` nel piè di pagina. Questo tipo di evento non è supportato da Amazon Pinpoint.

- Open and click tracking (Tracciamento aperture e clic): per misurare il coinvolgimento degli abbonati, scegli una o entrambe le caselle di controllo per tenere traccia di Opens (Aperture) e Clicks (Clic).
  - Opens (Aperture): il destinatario ha ricevuto il messaggio e lo ha aperto nel suo client e-mail.
  - Clicks (Clic): il destinatario ha fatto clic su uno o più collegamenti contenuti nell'e-mail.

> **Note**
>
> La pubblicazione dell'evento di apertura e clic definita qui, o in qualsiasi altro set di configurazione, non influisce sulle opzioni di monitoraggio del coinvolgimento per la dashboard di Virtual Deliverability Manager; queste vengono definite tramite le impostazioni dell'account di Virtual Deliverability Manager o le sostituzioni dei set di configurazione. Ad esempio, se il monitoraggio del coinvolgimento tramite Virtual Deliverability Manager è stato disattivato, la pubblicazione degli eventi di apertura e clic impostata qui non verrà disattivata nelle destinazioni degli eventi SES.

- Configuration set redirect domain (Dominio di reindirizzamento del set di configurazione): questo campo verrà visualizzato e prepopolato con il nome del dominio di reindirizzamento personalizzato, se ne hai assegnato uno durante la creazione del set di configurazione.

> **Note**
>
> È possibile aggiornare il Custom redirect domain (Dominio di reindirizzamento personalizzato) nel set di configurazione per il monitoraggio di apertura e clic in tale dominio; consulta Opzioni di monitoraggio nella Fase 4 di Creazione di set di configurazione. Per ulteriori informazioni sulla configurazione dei domini personalizzati di apertura e clic, consulta Configurazione di domini personalizzati per gestire il monitoraggio di aperture e clic.

b. Seleziona Next (Successivo) per continuare.

7. Specifica della destinazione

Una destinazione di eventi è un AWS servizio su cui è possibile pubblicare eventi di invio di e-mail. La scelta della destinazione appropriata dipende dal livello di dettaglio che si desidera acquisire e dal modo in cui si desidera ricevere i dati.

a. Opzioni di destinazione

- Tipo di destinazione: quando si seleziona il pulsante di opzione accanto al AWS servizio su cui pubblicare gli eventi, viene visualizzato un pannello dei dettagli con i campi relativi

al servizio. Selezionando i collegamenti riportati di seguito verranno fornite istruzioni sul pannello di dettaglio del servizio:

- Amazon CloudWatch (si applicano costi aggiuntivi, consulta Prezzo per metrica per CloudWatch.)
- Amazon Data Firehose
- Amazon EventBridge
- Amazon Pinpoint (non supporta i tipi di evento Delivery delays (Ritardi di consegna) o Subscriptions (Sottoscrizioni)).
- Amazon SNS

Per ulteriori informazioni sull'utilizzo del modello di pubblicazione degli eventi per monitorare le operazioni di e-mail, consulta Monitoraggio dell'invio di e-mail utilizzando la pubblicazione di eventi di Amazon SES.

- Name (Nome): immetti il nome della destinazione per questo set di configurazione. Il nome può includere solo lettere, numeri e trattini.
- Event publishing (Pubblicazione degli eventi): per attivare la pubblicazione di eventi per questa destinazione, seleziona la casella di controllo Enabled (Abilitato).

b. Seleziona Successivo per continuare.

8. Verificare

   Se le voci sono corrette, scegli Add destination (Aggiungi destinazione) per aggiungere la destinazione degli eventi.

È inoltre possibile creare una destinazione di eventi utilizzando la console Amazon SES, l'API Amazon SES v2 oppure Amazon SES CLI v2.

Per creare una destinazione di eventi utilizzando l'API SES:

- Per creare una destinazione di eventi utilizzando l'API SES, vedere `CreateConfigurationSetEventDestination`.

Modifica, abilitazione/disabilitazione o eliminazione di una destinazione degli eventi

Segui questi passaggi per modificare, disabilitare/abilitare o eliminare una destinazione di eventi utilizzando la console SES:

Per modificare, disabilitare/abilitare o eliminare una destinazione di eventi utilizzando la console SES:

1. Accedi AWS Management Console e apri la console Amazon SES all'indirizzo https://console.aws.amazon.com/ses/.
2. Nel pannello di navigazione, in Configuration (Configurazione), scegli Configuration sets (Set di configurazione).
3. Scegli il nome di un set di configurazione dalla colonna Nome per accedere ai suoi dettagli.
4. Seleziona la scheda del set di configurazione Destinazioni degli eventi.
5. Seleziona il nome della destinazione dell'evento nella colonna Nome.
6.
   - Per modificare - Scegli il pulsante Edit (Modifica) sul rispettivo pannello per il set di campi da modificare e apporta le modifiche seguite daSave changes (Salva le modifiche).
   - Per disabilitare o abilitare - Scegli il pulsante etichettato Disable (Disabilita) o Enable (Abilita) nella parte superiore destra.
   - Per eliminare- Scegli il pulsante Delete (Elimina) nella parte superiore destra.

Puoi anche modificare, disabilitare/abilitare o eliminare una destinazione di eventi utilizzando la console Amazon SES, l'API Amazon SES v2 oppure Amazon SES CLI v2.

Per modificare, disabilitare/abilitare o eliminare una destinazione di eventi utilizzando l'API SES:

1. Per disabilitare/abilitare una destinazione di eventi utilizzando l'API SES, vedere `UpdateConfigurationSetEventDestination`.
2. Per eliminare una destinazione di eventi utilizzando l'API SES, vedere `DeleteConfigurationSetEventDestination`.

Assegnazione di pool di IP in Amazon SES

I pool di IP permettono di creare gruppi di indirizzi IP dedicati per l'invio di specifici tipi di e-mail. Puoi anche usare un pool di indirizzi IP condivisi da tutti i clienti Amazon SES.

Quando assegni un pool di IP a un set di configurazione, puoi scegliere tra le seguenti opzioni:

- Un pool di IP dedicati specifici: quando selezioni un pool di indirizzi P dedicati esistenti, le e-mail che usano il set di configurazione vengono inviate utilizzando solo gli indirizzi IP dedicati che appartengono al pool. Per le procedure su come creare:

  - Nuovi pool IP standard, consulta Creazione di pool IP dedicati standard per IP dedicati (standard).
  - Nuovi pool di IP gestiti, consulta Creazione di un pool di IP gestiti per abilitare gli IP dedicati (gestiti).
- ses-default-dedicated-pool: questo pool contiene tutti gli indirizzi IP dedicati per il tuo account che non fanno già parte di un pool. Se invii un'e-mail utilizzando un set di configurazione che non è associato a un pool o se invii un'e-mail senza specificare un set di configurazione, l'e-mail viene inviata da uno degli indirizzi in questo pool predefinito. Questo pool è gestito automaticamente da SES e non può essere modificato.
- ses-shared-pool: questo pool contiene un ampio set di indirizzi IP condivisi tra tutti i clienti Amazon SES. Questa opzione può essere utile quando è necessario inviare e-mail non compatibili con i comportamenti di invio consueti.

Assegnazione di un pool di IP a un set di configurazione

Questa sezione fa riferimento alle procedure per l'assegnazione e la modifica dei pool di IP in un set di configurazione utilizzando la console Amazon SES.

- Per assegnare un pool di IP a un set di configurazione utilizzando la console…
  - durante la creazione di un nuovo set di configurazione, consulta Pool di IP Di invio nella fase 4 di Creazione di set di configurazione
  - durante la modifica di un set di configurazione esistente: seleziona il pulsante Edit (Modifica) nel pannello General details (Dettagli generali) del set di configurazione selezionato e segui le indicazioni per Sending IP pool (Pool di IP di invio) nella fase 4 di Creazione di set di configurazione

Configurazione di domini personalizzati per gestire il monitoraggio di aperture e clic

Quando utilizzi la pubblicazione di eventi per acquisire eventi di apertura e clic, Amazon SES apporta modifiche secondarie alle e-mail inviate. Per catturare eventi aperti, SES aggiunge un'immagine GIF trasparente da 1 pixel per 1 pixel in ogni e-mail inviata tramite SES che include un nome di file univoco per ogni e-mail ed è ospitata su un server gestito da SES; quando l'immagine viene scaricata, SES può indicare esattamente quale messaggio è stato aperto e da chi.

Di default, questo pixel viene inserito nella parte inferiore dell'e-mail; tuttavia, alcune applicazioni dei provider di posta elettronica troncano l'anteprima di un'e-mail quando supera una certa dimensione e potrebbero fornire un collegamento per visualizzare il resto del messaggio. In questo scenario, l'immagine di tracciamento dei pixel SES non viene caricata ed eliminerà le percentuali di aperture che stai cercando di tracciare. Per aggirare questo problema, puoi opzionalmente posizionare il pixel all'inizio dell'e-mail o in qualsiasi altro luogo inserendo il segnaposto `{{ses:openTracker}}` nel corpo dell'e-mail. Una volta che SES riceve il messaggio con il segnaposto, verrà sostituito con l'immagine pixel di tracciamento aperta.

> **Important**
>
> Aggiungi un solo segnaposto `{{ses:openTracker}}`, poiché più di un segnaposto genererà la restituzione di un codice di errore `400 BadRequestException`.

Per acquisire eventi di clic su collegamenti, Amazon SES sostituisce i collegamenti delle e-mail con collegamenti di un server gestito da Amazon SES. Questo reindirizza immediatamente il destinatario alla destinazione prevista.

È inoltre possibile utilizzare i propri domini, piuttosto che domini di proprietà e gestiti da Amazon SES, al fine di creare un'esperienza più coesa per i tuoi destinatari, il che significa che tutti gli indicatori SES vengono rimossi. Puoi configurare più domini personalizzati per gestire eventi di traccia di aperture e clic. Tali domini personalizzati sono associati ai set di configurazione. Quando invii un'e-mail tramite un set di configurazione, se quest'ultimo è configurato per l'utilizzo di un dominio personalizzato, i collegamenti di apertura e clic di quell'e-mail utilizzeranno automaticamente il dominio personalizzato specificato nel set di configurazione.

Questa sezione contiene le procedure di configurazione di un sottodominio su un server di tua proprietà per reindirizzare automaticamente gli utenti ai server di traccia di apertura e clic gestiti da Amazon SES. La configurazione di questi domini comprende tre fasi. In primo luogo, puoi configurare il sottodominio stesso, in seguito puoi impostare un set di configurazione per utilizzare il dominio personalizzato e poi impostare la destinazione dell'evento per pubblicare eventi aperti e di clic. Questo argomento contiene le procedure per completare entrambe le fasi.

Tuttavia, se si desidera semplicemente abilitare il tracciamento aperto o clic senza impostare un dominio personalizzato, è possibile procedere direttamente alla definizione delle destinazioni degli eventi per il set di configurazione che consente la pubblicazione di eventi attivata sui tipi di eventi specificati, inclusi gli eventi aperti e clic. Un set di configurazione può avere più destinazioni di eventi

con più tipi di eventi definiti. Per informazioni, consulta Creazione delle destinazioni degli eventi Amazon SES.

Fase 1: configurazione di un dominio per gestire i reindirizzamenti ai collegamenti di tracciamento di apertura e clic

Le procedure specifiche di configurazione di un dominio di reindirizzamento variano a seconda del provider di hosting Web (e della rete per la distribuzione di contenuti, se utilizzi un server HTTPS). Le procedure descritte nelle sezioni seguenti rappresentano indicazioni generali, piuttosto che fasi specifiche.

Opzione 1: configurazione di un dominio HTTP

Se intendi utilizzare un dominio HTTP per gestire i collegamenti di apertura e clic (anziché un dominio HTTPS), il processo di configurazione del sottodominio richiede solo pochi passaggi.

> **Note**
>
> Se configuri un dominio personalizzato che utilizza il protocollo HTTP e invii un'e-mail contenente collegamenti che utilizzano il protocollo HTTPS, i tuoi clienti potrebbero visualizzare un messaggio di avviso quando fanno clic sul collegamento contenuto nell'e-mail. Se intendi inviare e-mail contenenti collegamenti che utilizzano il protocollo HTTPS, è consigliabile utilizzare un dominio HTTPS per gestire gli eventi di tracciamento di clic.

Configurazione di un sottodominio HTTP per gestire i collegamenti di apertura e clic

1. Se non l'hai già fatto, crea un sottodominio da utilizzare per i collegamenti di traccia di apertura e clic. Ti consigliamo di creare un sottodominio dedicato nello specifico alla gestione di questi collegamenti.
2. Verifica il sottodominio per l'uso con Amazon SES. Per ulteriori informazioni, consulta Creazione di un'identità dominio.
3. Modifica il record DNS per il sottodominio. Nel record DNS, aggiungi un nuovo record CNAME che reindirizza le richieste verso il dominio di tracciamento di Amazon SES. L'indirizzo a cui reindirizzare dipende dalla AWS regione in cui utilizzi Amazon SES. La tabella seguente contiene un elenco dei domini di tracciamento per le regioni AWS in cui Amazon SES è disponibile.

AWS Regione	AWS dominio di tracciamento
Stati Uniti orientali (Ohio)	`r.us-east-2.awstrack.me`
Stati Uniti orientali (Virginia settentrionale)	`r.us-east-1.awstrack.me`
Stati Uniti occidentali (California settentrionale)	`r.us-west-1.awstrack.me`
Stati Uniti occidentali (Oregon)	`r.us-west-2.awstrack.me`
Africa (Città del Capo)	`r.af-south-1.awstrack.me`
Asia Pacifico (Giacarta)	`r.ap-southeast-3.awstrack.me`
Asia Pacifico (Mumbai)	`r.ap-south-1.awstrack.me`
Asia Pacific (Osaka)	`r.ap-northeast-3.awstrack.me`
Asia Pacific (Seul)	`r.ap-northeast-2.awstrack.me`
Asia Pacifico (Singapore)	`r.ap-southeast-1.awstrack.me`
Asia Pacifico (Sydney)	`r.ap-southeast-2.awstrack.me`
Asia Pacifico (Giacarta)	r.ap-southeast-3.awstrack.me
Asia Pacifico (Giacarta)	r.ap-southeast-3.awstrack.me
Asia Pacifico (Tokyo)	`r.ap-northeast-1.awstrack.me`
Canada (Centrale)	`r.ca-central-1.awstrack.me`
Europa (Francoforte)	`r.eu-central-1.awstrack.me`
Europa (Irlanda)	`r.eu-west-1.awstrack.me`
Europa (Londra)	`r.eu-west-2.awstrack.me`
Europa (Milano)	`r.eu-south-1.awstrack.me`

AWS Regione	AWS dominio di tracciamento
Europa (Stoccolma)	`r.eu-north-1.awstrack.me`
Israele (Tel Aviv)	`r.il-central-1.awstrack.me`
Medio Oriente (Bahrein)	`r.me-south-1.awstrack.me`
Sud America (San Paolo)	`r.sa-east-1.awstrack.me`
AWS GovCloud (Stati Uniti occidentali)	`r.us-gov-west-1.awstrack.me`
AWS GovCloud (Stati Uniti orientali)	`r.us-gov-east-1.awstrack.me`

> **Note**
>
> A seconda del provider di hosting Web, potrebbero essere necessari alcuni minuti perché le modifiche apportate al record DNS del sottodominio siano effettive. Il tuo provider di hosting Web o l'organizzazione IT può fornire ulteriori informazioni relative a questi ritardi.

Opzione 2: configurazione di un dominio HTTPS

Puoi utilizzare solo un dominio HTTPS per tenere traccia dei clic dei collegamenti. Per configurare un dominio HTTPS per il monitoraggio dei clic dei collegamenti, è necessario eseguire alcune fasi aggiuntive, oltre a quelle richieste per configurare un dominio HTTP.

> **Note**
>
> Puoi utilizzare solo un dominio HTTPS per tenere traccia dei clic dei collegamenti. Amazon SES supporta il monitoraggio delle aperture su domini HTTP solo quando si utilizza un dominio personalizzato; quando non è definito un dominio personalizzato, invece, SES supporta il monitoraggio delle aperture su HTTPS, che utilizza implicitamente domini di proprietà e gestiti da SES.

Configurazione di un sottodominio HTTPS per gestire i collegamenti dei clic

1. Crea un sottodominio da utilizzare per monitorare i clic dei collegamenti. Ti consigliamo di creare un sottodominio dedicato nello specifico alla gestione di questi collegamenti.
2. Verifica il sottodominio per l'uso con Amazon SES. Per ulteriori informazioni, consulta Creazione di un'identità dominio.
3. Crea un nuovo account con un Content Delivery Network (CDN), come Amazon CloudFront.
4. Configura il CDN sull'origine che è il dominio di tracciamento SES, ad esempio `r.us-east-1.awstrack.me`. Il CDN deve passare l'intestazione `Host` fornita dal richiedente all'origine. Fai riferimento a questo articolo di AWS Re:POST per ulteriori informazioni. L'indirizzo che usi dipende da Regione AWS quello che usi in SES. La tabella seguente contiene un elenco di domini di tracciamento per le AWS regioni in cui è disponibile SES.

AWS Regione	AWS dominio di tracciamento
Stati Uniti orientali (Ohio)	`r.us-east-2.awstrack.me`
Stati Uniti orientali (Virginia settentrionale)	`r.us-east-1.awstrack.me`
Stati Uniti occidentali (California settentrionale)	`r.us-west-1.awstrack.me`
Stati Uniti occidentali (Oregon)	`r.us-west-2.awstrack.me`
Africa (Città del Capo)	`r.af-south-1.awstrack.me`
Asia Pacifico (Giacarta)	`r.ap-southeast-3.awstrack.me`
Asia Pacifico (Mumbai)	`r.ap-south-1.awstrack.me`
Asia Pacific (Osaka)	`r.ap-northeast-3.awstrack.me`
Asia Pacific (Seul)	`r.ap-northeast-2.awstrack.me`
Asia Pacifico (Singapore)	`r.ap-southeast-1.awstrack.me`
Asia Pacifico (Sydney)	`r.ap-southeast-2.awstrack.me`
Asia Pacifico (Tokyo)	`r.ap-northeast-1.awstrack.me`

AWS Regione	AWS dominio di tracciamento
Canada (Centrale)	`r.ca-central-1.awstrack.me`
Europa (Francoforte)	`r.eu-central-1.awstrack.me`
Europa (Irlanda)	`r.eu-west-1.awstrack.me`
Europa (Londra)	`r.eu-west-2.awstrack.me`
Europa (Milano)	`r.eu-south-1.awstrack.me`
Europa (Stoccolma)	`r.eu-north-1.awstrack.me`
Israele (Tel Aviv)	`r.il-central-1.awstrack.me`
Medio Oriente (Bahrein)	`r.me-south-1.awstrack.me`
Sud America (San Paolo)	`r.sa-east-1.awstrack.me`
AWS GovCloud (Stati Uniti occidentali)	`r.us-gov-west-1.awstrack.me`
AWS GovCloud (Stati Uniti orientali)	`r.us-gov-east-1.awstrack.me`

5. Se utilizzi Route 53 per gestire la configurazione DNS per il tuo dominio e CloudFront come CDN, crea un record di alias in Route 53 che faccia riferimento alla tua CloudFront distribuzione (ad esempio d111111abcdef8.cloudfront.net). Per maggiori informazioni, consulta Creazione di registro utilizzando la console Amazon Route 53 nella Guida per gli sviluppatori Amazon Route 53.

   In caso contrario, nella configurazione DNS per il tuo sottodominio, aggiungi un record CNAME che faccia riferimento all'indirizzo della tua CDN.

6. Acquisisci un certificato SSL da un'autorità di certificazione attendibile. Il certificato dovrebbe coprire sia il sottodominio creato nella fase 1, sia la CDN è configurata nelle fasi 3-5. Carica il certificato nella CDN.

Fase 2: impostazione di un set di configurazione per fare riferimento a un dominio di tracciamento di apertura e clic personalizzato

Dopo aver configurato il dominio per gestire i reindirizzamenti di tracciamento di apertura e clic, è necessario configurare una destinazione di eventi in un set di configurazione. Puoi completare questa fase utilizzando la console Amazon SES o l'operazione API `CreateConfigurationSetTrackingOptions`.

Questa sezione fa riferimento alle procedure per completare queste attività utilizzando la console Amazon SES. Per informazioni sull'uso dell'API, consulta CreateConfigurationSetTrackingOpzioni nel riferimento all'API di Amazon Simple Email Service.

- Per specificare un dominio di reindirizzamento personalizzato tramite la console...
  - durante la creazione di un nuovo set di configurazione, consulta Opzioni di monitoraggio nella fase 4 di Creazione di set di configurazione
  - durante la modifica di un set di configurazione esistente: seleziona il pulsante Edit (Modifica) nel pannello General details (Dettagli generali) del set di configurazione selezionato e segui le indicazioni per Tracking options (Opzioni di monitoraggio) nella fase 4 di Creazione di set di configurazione

Parte 3: selezione dei tipi di eventi apertura e clic nelle destinazioni degli eventi del set di configurazione

Dopo aver specificato il dominio personalizzato nel set di configurazione, è necessario selezionare i tipi di evento apertura e/o clic in una destinazione di evento aggiunta al set di configurazione. Puoi completare questa fase utilizzando la console Amazon SES o l'operazione API `CreateConfigurationSetEventDestination`.

- Per selezionare i tipi di eventi apertura e/o clic utilizzando la console...
  - durante la creazione di una nuova destinazione di eventi - consulta Monitoraggio di apertura e clic nella fase 6 di the section called “Creazione di una destinazione degli eventi”.
  - durante la modifica di una destinazione di eventi esistente - selezionare il pulsante Edit (Modifica) nel pannello Tipi di eventi della destinazione dell'evento selezionata nel passaggio 6 di the section called “Modifica, abilitazione/disabilitazione o eliminazione di una destinazione degli eventi”

Specifica di un set di configurazione per l'invio di e-mail

Per usare un set di configurazione durante l'invio di un'e-mail, devi passare il nome del set di configurazione nelle intestazioni dell'e-mail. Tutti i metodi di invio di e-mail di Amazon SES, tra cui la AWS CLI, gli SDK AWS e l'interfaccia SMTP di Amazon SES, consentono di passare un set di configurazione nelle intestazioni dell'e-mail che invii.

Se utilizzi l'interfaccia SMTP o l'operazione API `SendRawEmail`, puoi specificare un set di configurazione includendo l'intestazione seguente nella tua e-mail, sostituendo *`ConfigSet`* con il nome del set di configurazione che desideri utilizzare:

```
X-SES-CONFIGURATION-SET: ConfigSet
```

Questa guida include esempi di codice per l'invio di e-mail usando gli AWS SDK e l'interfaccia SMTP Amazon SES. Ogni esempio include un metodo per specificare un set di configurazione. Per visualizzare step-by-step le procedure per l'invio di e-mail che includono riferimenti ai set di configurazione, consulta quanto segue:

- Invio di e-mail tramite Amazon SES utilizzando un AWS SDK
- Utilizzo dell'interfaccia SMTP Amazon SES per inviare e-mail

Visualizzazione ed esportazione dei parametri di reputazione

Amazon SES esporta automaticamente le informazioni sulle percentuali complessive di rimbalzo e di reclamo per l'intero account su Amazon. CloudWatch Puoi utilizzare queste metriche per creare allarmi o per sospendere automaticamente l'invio di e-mail utilizzando una funzione Lambda. CloudWatch

Puoi anche esportare le metriche di reputazione per singoli set di configurazione in. CloudWatch L'esportazione dei dati i reputazione a livello di set di configurazione fornisce maggiore controllo sulla reputazione del mittente.

Questa sezione include le procedure per esportare i dati di reputazione per singoli set di configurazione CloudWatch utilizzando l'API Amazon SES.

Abilitazione dell'esportazione dei parametri di reputazione

Per avviare l'esportazione dei parametri di reputazione per un set di configurazione, usa l'operazione API `UpdateConfigurationSetReputationMetricsEnabled`. Per accedere all'API Amazon SES, consigliamo di utilizzare lo AWS CLI o uno degli AWS SDK.

Questa procedura presuppone che AWS CLI sia installato sul tuo computer e configurato correttamente. Per ulteriori informazioni sull'installazione e la configurazione di AWS CLI, consultare la Guida per l'AWS Command Line Interface utente.

Abilitazione dell'esportazione dei parametri di reputazione per un set di configurazione

- Nella riga di comando, digita il comando seguente:

```
aws ses update-configuration-set-reputation-metrics-enabled --configuration-set-
name ConfigSet --enabled
```

  *ConfigSet*Sostituitelo nel comando precedente con il nome del set di configurazione per il quale desiderate iniziare a esportare le metriche di reputazione.

Disabilitazione dell'esportazione dei parametri di reputazione

L'operazione API `UpdateConfigurationSetReputationMetricsEnabled` permette inoltre di disabilitare l'esportazione dei parametri di reputazione per un set di configurazione.

Disabilitazione dell'esportazione dei parametri di reputazione per un set di configurazione

- Nella riga di comando, digita il comando seguente:

```
aws ses update-configuration-set-reputation-metrics-enabled --configuration-set-
name ConfigSet --no-enabled
```

  Sostituitelo *ConfigSet*nel comando precedente con il nome del set di configurazione per il quale desiderate disabilitare l'esportazione delle metriche di reputazione.

Indirizzi IP dedicati per Amazon SES

Quando viene creato un nuovo account Amazon SES, le e-mail vengono inviate da indirizzi IP condivisi con altri utenti di Amazon SES. Per un costo supplementare, è possibile utilizzare indirizzi IP dedicati riservati all'uso esclusivo mediante il noleggio. Questo darà il controllo completo sulla reputazione del mittente e consentirà di isolare la reputazione per diversi segmenti all'interno dei programmi di e-mail. In Amazon SES sono disponibili due modi per effettuare il provisioning e gestire un indirizzo IP dedicato:

- Standard: si riferisce agli indirizzi IP dedicati impostati e gestiti manualmente, inclusa la possibilità di prepararli e aumentarli orizzontalmente in modo manuale e di spostarli manualmente dentro e fuori dai pool di IP. (Sono stati formalmente denominati indirizzi IP dedicati in SES.)
- Managed (Gestito): si riferisce agli indirizzi IP dedicati che vengono impostati automaticamente per conto dell'utente da SES per fornire un modo semplice e rapido per iniziare a utilizzare indirizzi IP dedicati gestiti da SES; vengono automaticamente preparati per ogni fornitore di servizi Internet (ISP) individualmente e si ridimensionano automaticamente in base al volume di invio per garantire che gli indirizzi IP dedicati vengano utilizzati in modo ottimale in base alla modalità di invio delle e-mail.

Quando devi decidere tra indirizzi IP condivisi o indirizzi IP dedicati definiti sopra, scegli il tipo di indirizzo che offre maggiori vantaggi in base al tipo, al volume e ai modelli di e-mail che invii. A supporto della decisione da prendere, nella tabella seguente sono riepilogati i vari vantaggi. Scegli una voce nella colonna Vantaggi per ulteriori informazioni.

Vantaggio	Indirizzi IP condivisi	Indirizzi IP dedicati (standard)	Indirizzi IP dedicati (gestiti)
Pronto all'uso immediato	Sì	No	No
È richiesta una configurazione aggiuntiva	No	Sì	Sì

Vantaggio	Indirizzi IP condivisi	Indirizzi IP dedicati (standard)	Indirizzi IP dedicati (gestiti)
Indirizzi IP e reputazione isolati dagli altri clienti SES	No	Sì	Sì
La capacità aumenta automaticamente all'aumentare del traffico	No	No	Sì
Ideali per i clienti con modelli di invio continui, prevedibili	Sì	Sì	Sì
Ideali per i clienti con modelli di invio meno prevedibili	Sì	No	Sì
Ideali per mittenti di volumi elevati	Sì	Sì	Sì
Ideali per mittenti di volumi ridotti	Sì	No	No
Costi mensili supplementari	No	Sì	Sì
Controllo completo della reputazione del mittente	No	Sì	Sì
Isolamento della reputazione per tipo di e-mail, destinatario o altri fattori	No	Sì	Sì

Vantaggio	Indirizzi IP condivisi	Indirizzi IP dedicati (standard)	Indirizzi IP dedicati (gestiti)
Indirizzi IP noti che non cambiano mai	No	Sì	No

> **Important**
>
> Se non prevedi di inviare grandi volumi di posta elettronica su base regolare e prevedibile, ti consigliamo di utilizzare indirizzi IP condivisi. Se desideri utilizzare indirizzi IP dedicati in situazioni in cui i modelli di invio sono estremamente irregolari, si consiglia di utilizzare gli IP dedicati (gestiti).

Semplicità di configurazione

Indirizzi IP condivisi: non è necessario eseguire configurazione aggiuntiva. L'account SES è pronto per inviare e-mail non appena avrai verificato un indirizzo e-mail e sarai uscito dalla sandbox (ambiente di sperimentazione).

Indirizzi IP dedicati (standard): è necessario inviare una richiesta tramite il AWS Support Center e, facoltativamente, configurare pool IP dedicati.

Indirizzi IP dedicati (gestiti): non è necessario inviare una richiesta di indirizzi IP dedicati. Verranno allocati automaticamente quando effettui l'iscrizione ed esegui una procedura dettagliata una tantum per creare il pool dedicato gestito.

Gestione della reputazione

Le reputazioni degli indirizzi IP sono ampiamente basate su volume e modelli di invio storici. Un indirizzo IP che invia volumi di posta elettronica uniformi per un lungo periodo gode in genere di una buona reputazione.

Indirizzi IP condivisi: condivisi tra diversi clienti SES, questi indirizzi inviano collettivamente un grande volume di e-mail; AWS gestisce con attenzione il traffico in uscita per massimizzare la reputazione degli indirizzi IP condivisi.

Indirizzi IP dedicati (standard): dopo il riscaldamento, gli indirizzi IP vengono isolati dal pool condiviso SES e l'utente mantiene la propria reputazione di mittente inviando volumi di e-mail coerenti e prevedibili.

Indirizzi IP dedicati (gestiti): dopo il riscaldamento dei nuovi IP, vengono isolati dal pool condiviso SES e tu mantieni la tua reputazione di mittente. C'è l'ulteriore vantaggio di monitorare la reputazione di ogni ISP e di pianificare in modo ottimale l'invio in uscita di conseguenza. Quindi, pur mantenendo la reputazione del mittente, questa automazione aiuta a migliorare la consegna complessiva e a ridurre le frequenze di mancato recapito rispetto ai carichi di lavoro equivalenti su indirizzi IP dedicati configurati manualmente.

> **Note**
>
> Per informazioni sui dati SNDS (Smart Network Data Services) per gli IP dedicati, consulta Parametri SNDS per gli indirizzi IP dedicati.

Prevedibilità dei modelli di invio

Un indirizzo IP con una cronologia di invio di posta elettronica uniforme ha una migliore reputazione rispetto a uno che inizia improvvisamente a inviare grandi volumi di posta in assenza di una precedente cronologia di invio.

Indirizzi IP condivisi: adatti per schemi di invio di e-mail che non seguono uno schema prevedibile. Con gli indirizzi IP condivisi, puoi aumentare o diminuire i modelli di invio di e-mail in funzione delle circostanze.

Indirizzi IP dedicati (standard): è necessario preparare gli indirizzi inviando una quantità di e-mail che aumenti gradualmente ogni giorno. Il processo di preparazione di nuovi indirizzi IP viene descritto in Preparazione di indirizzi IP dedicati (standard). Dopo aver preparato gli indirizzi IP dedicati, è necessario mantenere un modello di invio uniforme.

Indirizzi IP dedicati (gestiti): gli indirizzi IP dedicati vengono riscaldati automaticamente per ogni IP del pool gestito utilizzando una strategia di riscaldamento adattiva (in combinazione con il pool condiviso SES) che tiene conto degli schemi di invio effettivi per ottimizzare il riscaldamento di ciascun ISP individualmente. Il pool IP gestito si ridimensiona automaticamente per ogni ISP in base all'utilizzo e alla considerazione delle politiche specifiche dell'ISP.

Volume di posta elettronica in uscita

Indirizzi IP condivisi: adatti per i clienti che inviano bassi volumi di e-mail.

Indirizzi IP dedicati (standard) | Indirizzi IP dedicati (gestiti): entrambi sono adatti per clienti che inviano grandi volumi di e-mail. La maggior parte dei fornitori di servizi Internet (ISP) tiene traccia solo della reputazione di un determinato indirizzo IP da cui riceve un notevole volume di posta. Per ogni ISP con cui desideri coltivare una reputazione, è necessario inviare diverse centinaia di e-mail entro un periodo di 24 ore almeno una volta al mese. In alcuni casi, entrambi i tipi di indirizzi IP dedicati possono funzionare anche per volumi di e-mail più piccoli. Ad esempio, possono funzionare perfettamente in caso di invio a un piccolo e ben definito gruppo di destinatari i cui server di posta accettano o rifiutano e-mail utilizzando un elenco di indirizzi IP specifici anziché la loro reputazione.

Costi aggiuntivi

Indirizzi IP condivisi: sono inclusi nel prezzo SES standard.

Indirizzi IP dedicati (standard): sono disponibili a un costo mensile aggiuntivo per ogni indirizzo IP noleggiato. Per informazioni sui prezzi, consulta la pagina dei prezzi di SES.

Indirizzi IP dedicati (gestiti): sono disponibili con una tariffa mensile standard (indipendentemente dalla quantità di IP necessaria) e con un costo di utilizzo per messaggio. Per informazioni sui prezzi, consulta la pagina dei prezzi di SES.

Controllo della reputazione del mittente

Indirizzi IP condivisi: la reputazione del mittente è controllata da SES.

Indirizzi IP dedicati (standard) | Indirizzi IP dedicati (gestiti): la reputazione del mittente è completamente sotto il tuo controllo. L'account SES è l'unico in grado di inviare e-mail da tali indirizzi. Per questo motivo, la reputazione del mittente viene determinata sulla base delle best practice di invio di e-mail. Inoltre, gli IP dedicati (gestiti) monitorano attivamente gli indirizzi IP in uscita utilizzati per l'invio di e-mail utilizzando gli indirizzi IP con le prestazioni più elevate per migliorare la consegna delle e-mail ai destinatari. I dati di utilizzo possono essere visualizzati utilizzando servizi aggiuntivi come i CloudWatch parametri di Amazon e le dashboard integrate presenti in Amazon SES.

Capacità di isolamento della reputazione di mittente

Indirizzi IP condivisi: la reputazione del mittente è impostata a livello di account e non può essere isolata.

Indirizzi IP dedicati (standard) | Indirizzi IP dedicati (gestiti): è possibile isolare la reputazione del mittente per i diversi componenti del programma e-mail creando pool di IP dedicati, ossia gruppi di indirizzi IP dedicati che possono essere utilizzati per l'invio di determinati tipi di e-mail. Ad esempio, puoi creare un pool di indirizzi IP dedicati per l'invio di e-mail di marketing e un'altra per l'invio di e-mail transazionali.

Indirizzi IP noti e statici

Indirizzi IP condivisi: gli indirizzi IP usati da SES per l'invio della posta non sono noti e possono cambiare in qualsiasi momento.

Indirizzi IP dedicati (standard): i valori degli indirizzi che inviano le e-mail sono disponibili nella pagina Dedicated IPs (IP dedicati) della console SES. Ciò è dovuto al fatto che gli indirizzi IP dedicati sono statici.

Indirizzi IP dedicati (gestiti): SES configurerà automaticamente il numero ottimale di indirizzi IP dedicati in base ai modelli di invio. Ciò significa che gli indirizzi IP dedicati nel pool non sono visibili e aumenteranno o diminuiranno dinamicamente in base alla domanda.

Indirizzi IP dedicati (standard) per Amazon SES

Gli indirizzi IP dedicati (standard) sono indirizzi IP dedicati configurati e gestiti manualmente in SES. Sono diversi da quelli configurati e gestiti automaticamente utilizzando la funzione SES the section called “Gestiti”. Oltre a consentire il controllo totale sulla reputazione di invio tramite indirizzi IP dedicati, gli IP dedicati (standard) consentono di gestire completamente gli IP dedicati, inclusi la preparazione, il dimensionamento e la gestione del pool di IP.

Gli IP dedicati (standard) e gli IP dedicati (gestiti) si riferiscono entrambi a indirizzi IP dedicati noleggiati in SES a un prezzo aggiuntivo, ma differiscono nel modo in cui vengono implementati e gestiti. Sebbene condividano vantaggi comuni, ognuno di essi ha vantaggi unici da offrire a seconda del tipo di invio di e-mail, come descritto in Indirizzi IP dedicati.

Gli argomenti di questa sezione spiegano come configurare e gestire manualmente gli IP dedicati (standard) in SES.

Argomenti

Richiesta e rilascio di indirizzi IP dedicati (standard)

Per utilizzare indirizzi IP dedicati (standard), devi prima richiederli. Quando non sono più necessari, è consigliabile rilasciarli. È possibile richiedere e rilasciare gli IP dedicati (standard) tramite il Centro AWS Support. Sull'account viene addebitata una tariffa mensile aggiuntiva per ogni indirizzo IP dedicato standard noleggiato per l'uso con Amazon SES. Non è previsto un impegno minimo quando si utilizzano IP dedicati (standard).

Per ulteriori informazioni sui costi associati agli indirizzi IP dedicati (standard), consulta Prezzi di Amazon SES.

Per l'elenco di tutte le regioni nelle quali Amazon SES è disponibile, vedi Regione AWS ed endpoint in Riferimenti generali di Amazon Web Services. Per ulteriori informazioni sul numero di zone di disponibilità presenti in ciascuna Regione AWS, consulta Infrastruttura globale di AWS.

Richiesta di IP dedicati (standard)

È possibile richiedere tutti gli IP dedicati (standard) necessari creando un aumento delle Service Quotas nel Centro Supporto AWS.

Richiesta di IP dedicati (standard)

1. Accedi alla AWS Management Console e apri la console Amazon SES all'indirizzo https://console.aws.amazon.com/ses/.
2. Nel riquadro di navigazione a sinistra, scegli Dedicated IPs (IP dedicati).
3. Completa una delle seguenti operazioni:

    a. Se nel tuo account non sono già presenti IP dedicati:

    - Viene aperta la pagina di onboarding Dedicated IPs (IP dedicati). Nel pannello Dedicated IPs (standard) overview (Panoramica degli IP dedicati (standard)), scegli Request dedicated IPs (Richiedi IP dedicati).

Viene aperta la pagina Create case (Crea caso) nella Console di supporto AWS.

b. Se nel tuo account sono già presenti IP dedicati:

   i. Seleziona la scheda Standard IP pools (Pool IP standard) nella pagina Dedicated IPs (IP dedicati).

   ii. Nel pannello Standard overview (Panoramica standard), scegli Request or relinquish Standard dedicated IPs (Richiedi o rilascia IP dedicati standard).

   Viene aperta la pagina Create case (Crea caso) nella Console di supporto AWS.

4. In Create case (Crea caso), seleziona la scheda Service limit increase (Aumento dei limiti di servizio) nella parte superiore della pagina.
5. In Case details (Dettagli pratica), completa le seguenti sezioni:

   - Per Limit type (Tipo di limite), scegli SES Service Limits (Limiti del servizio SES).
   - Per Mail Type (Tipo di e-mail), scegli il tipo di e-mail che intendi inviare utilizzando l'indirizzo IP dedicato. Se si applicano più valori, scegli l'opzione adatta per la maggior parte delle e-mail che intendi inviare.
   - Per Website URL (URL sito Web), immetti l'URL del sito Web. Queste informazioni ci aiuteranno a comprendere meglio il tipo di contenuto che intendi inviare.
   - In Describe, in detail, how you will only send to recipients who have specifically requested your mail (Descrivi in dettaglio le modalità di invio solo ai destinatari che le hanno specificamente richieste), fornisci una risposta coerente con il caso d'uso.
   - In Describe, in detail, the process that you will follow when you receive bounce and complaint notifications (Descrivi in dettaglio la procedura da seguire quando ricevi notifiche di mancato recapito e reclami), fornisci una risposta coerente con il caso d'uso.
   - Per Will comply with the AWS Service Terms and AUP (Sarà conforme alle condizioni di servizio e alla policy di uso accettabile AWS), scegli l'opzione applicabile al caso d'uso.
6. In Requests (Richieste), completa le seguenti sezioni:

   - Per Region (Regione), scegli l'Regione AWS a cui si applica la richiesta.
   - In Limit (Limite), scegli Desired Dedicated IP (IP dedicato desiderato).
   - In New limit value (Nuovo valore limite), inserisci il numero di indirizzi IP dedicati necessari per implementare il caso d'uso.

> **Note**
>
> Se desideri richiedere indirizzi IP dedicati per l'uso in un'altra Regione AWS, scegli Add another request (Aggiungi altra richiesta) e completa i campi Region (Regione), Limit (Limite) e New limit value (Valore nuovo limite) per la Regione AWS aggiuntiva. Ripeti la procedura per ogni Regione AWS in cui desideri utilizzare gli indirizzi IP dedicati.

7. In Case description (Descrizione caso), per Use case description (Descrizione del caso d'uso), indica di voler richiedere indirizzi IP dedicati. Se desideri richiedere un determinato numero di indirizzi IP dedicati, indica il numero. Se non specifici un numero di indirizzi IP dedicati, verrà fornito il numero di indirizzi IP dedicati necessari per soddisfare il requisito relativo alla frequenza di invio specificato nel passaggio precedente.

   Quindi, descrivi come intendi usare gli indirizzi IP dedicati per l'invio di e-mail tramite Amazon SES. Includi le motivazioni dell'uso degli indirizzi IP dedicati anziché gli indirizzi IP condivisi. Queste informazioni aiutano a comprendere meglio il caso d'uso.
8. In Contact options (Opzioni di contatto), per Preferred contact language (Lingua di contatto preferita), scegliere se le comunicazioni ricevute devono essere in inglese o in giapponese.
9. Al termine, scegli Submit (Invia).

Una volta inviato il modulo, verrà valutata la richiesta. Se la richiesta viene approvata, rispondiamo alla pratica nel Centro di supporto per confermare che i nuovi indirizzi IP dedicati sono associati all'account.

Rilascio di indirizzi IP dedicati standard

Se utilizzi indirizzi IP dedicati e non desideri più che vengano associati al tuo account, la procedura seguente mostra come rilasciarli creando un caso nel Centro Supporto AWS.

> **Important**
>
> Il processo di rinuncia di un indirizzo IP dedicato non può essere annullato. Se rilasci a un indirizzo IP dedicato a metà mese, la tariffa di utilizzo mensile dell'IP dedicato verrà ripartita proporzionalmente in base al numero di giorni trascorsi nel mese corrente.

Rilascio di IP dedicati (standard)

1. Accedi alla AWS Management Console e apri la console Amazon SES all'indirizzo https://console.aws.amazon.com/ses/.
2. Nel riquadro di navigazione a sinistra, scegli Dedicated IPs (IP dedicati).
3. Seleziona la scheda Standard IP pools (Pool IP standard) nella pagina Dedicated IPs (IP dedicati).
4. Nel pannello Standard overview (Panoramica standard), scegli Request or relinquish Standard dedicated IPs (Richiedi o rilascia IP dedicati standard).
5. In Case details (Dettagli caso), per Limit type (Tipo di limite), scegli SES Service Limits (Limiti servizio SES).

> **Note**
>
> Le caselle rimanenti in questa sezione non si applicano alla procedura di rilascio degli IP dedicati. Lasciale vuote.

6. In Requests (Richieste), completa le seguenti sezioni:

   - In Region (Regione), scegli la Regione AWS interessata dalla richiesta di rilascio.

   > **Note**
   >
   > Gli indirizzi IP dedicati sono univoci per ogni Regione AWS e quindi è importante selezionare la Regione AWS a cui è associato l'indirizzo IP dedicato.

   - In Limit (Limite), scegli Desired Dedicated IP (IP dedicato desiderato).
   - In New limit value (Valore nuovo limite), immetti un numero qualsiasi. Il numero immesso non è importante: nel passaggio successivo è necessario specificare il numero di IP dedicati a cui si desidera rinunciare.

   > **Note**
   >
   > Puoi utilizzare un singolo indirizzo IP dedicato in una sola Regione AWS. Per rilasciare gli indirizzi IP dedicati utilizzati in altre Regioni AWS, scegli Add another request (Aggiungi altra richiesta). Quindi completa i campi Region (Regione), Limit (Limite) e New

limit value (Valore nuovo limite) per la Regione AWS aggiuntiva. Ripeti la procedura per ogni indirizzo IP dedicato a cui desideri rinunciare.

7. In Case Description (Descrizione caso), per Use case description (Descrizione del caso d'uso), indica di voler rinunciare agli indirizzi IP dedicati. Se al momento sono in leasing più indirizzi IP dedicati, includi il numero degli indirizzi IP dedicati da rinunciare.
8. In Contact options (Opzioni di contatto), per Preferred contact language (Lingua di contatto preferita), scegliere se le comunicazioni ricevute devono essere in inglese o in giapponese.
9. Al termine, scegli Submit (Invia).

Una volta ricevuta la tua richiesta, verrà inviato un messaggio per richiedere di confermare la rinuncia degli indirizzi IP dedicati. Dopo aver confermato la rinuncia, gli indirizzi IP vengono rimossi dall'account.

Preparazione di indirizzi IP dedicati (standard)

Quando stabiliscono se accettare o rifiutare un messaggio, i provider di servizi di posta elettronica considerano la reputazione dell'indirizzo IP che lo ha inviato. Uno dei fattori che contribuisce alla reputazione di un indirizzo IP è se l'indirizzo vanta una storia di invio di e-mail di alta qualità. I provider di servizi di posta elettronica sono poco inclini ad accettare posta da indirizzi IP nuovi che hanno una storia breve o nulla. Le e-mail inviate da questo tipo di indirizzi IP potrebbero finire nelle cartelle spam dei destinatari o bloccate in modo definitivo.

Quando inizi a inviare e-mail da un nuovo indirizzo IP dedicato, devi gradualmente aumentare il numero di e-mail inviate da tale indirizzo prima di utilizzarlo a piena capacità. Questo processo viene chiamato preparazione dell'indirizzo IP.

La quantità di tempo necessaria per preparare un indirizzo IP varia in base ai fornitori di servizi e-mail. In alcuni casi puoi stabilire una reputazione positiva in circa due settimane, mentre in altri potrebbero essere necessarie fino a sei settimane. Quando prepari un nuovo indirizzo IP dedicato, è consigliabile inviare e-mail agli utenti più attivi, in modo che la percentuale di reclami rimanga bassa. Dovresti anche analizzare con attenzione i mancati recapiti e inviare un numero minore di e-mail se ricevi un numero elevato di notifiche di blocco o throttling (limitazione). Per informazioni sul monitoraggio dei mancati recapiti, consulta Monitoraggio delle attività di invio di Amazon SES.

Preparazione automatica degli IP dedicati (standard)

Quando richiedi indirizzi IP dedicati (standard), Amazon SES li prepara automaticamente per migliorare la consegna delle e-mail inviate. La caratteristica di preparazione automatica degli indirizzi IP è abilitata per impostazione predefinita. SES prepara automaticamente gli IP dedicati aumentando gradualmente il numero di e-mail inviate tramite gli IP dedicati in base a un piano di preparazione predefinito. La quantità massima giornaliera di e-mail aumenta dal primo giorno fino a raggiungere un massimo di 50.000 e-mail entro 45 giorni. Questo aumento graduale consente gli IP di creare una reputazione positiva presso i fornitori di servizi Internet (ISP).

Le operazioni che si verificano durante il processo di preparazione automatica variano a seconda del fatto che gli indirizzi IP dedicati siano disponibili o meno:

- Quando richiedi IP dedicati (standard) per la prima volta, SES distribuisce l'attività di invio di e-mail tra gli indirizzi IP dedicati e un set di indirizzi condivisi con altri clienti SES. SES aumenta gradualmente il numero di messaggi inviati dagli indirizzi IP dedicati nel corso del tempo.
- Se disponi già di indirizzi IP dedicati, SES distribuisce l'attività di invio di e-mail tra gli indirizzi IP dedicati esistenti (già preparati) e quelli nuovi (non preparati). SES aumenta gradualmente il numero di messaggi inviati dai nuovi indirizzi IP dedicati nel corso del tempo.

> **Note**
>
> La preparazione automatica dell'IP è un processo basato sul tempo. La percentuale di preparazione aumenta costantemente in 45 giorni indipendentemente dal volume di invio.

Da un indirizzo IP dedicato preparato dovresti inviare circa 1.000 messaggi e-mail ogni giorno a ogni provider di servizi di posta elettronica presso cui desideri mantenere una reputazione positiva. Devi eseguire questa operazione per ciascun indirizzo IP dedicato che utilizzi con SES.

È consigliabile evitare l'invio di grandi volumi di e-mail subito dopo il completamento del processo di preparazione. Piuttosto, aumenta lentamente il numero di e-mail inviate fino a raggiungere il tuo obiettivo in termini di volume. Se un fornitore di servizi di e-mail vede un grande e improvviso aumento del numero di e-mail inviate da un indirizzo IP, potrebbe bloccare o limitare la consegna dei messaggi provenienti da quell'indirizzo.

Disabilitazione del processo di preparazione automatica su IP dedicati (standard)

Quando acquisti nuovi indirizzi IP dedicati standard, Amazon SES li prepara automaticamente perché la funzione di preparazione automatica degli indirizzi IP è abilitata per impostazione predefinita per l'account in uso. Se preferisci prepararli in autonomia, puoi disabilitare la funzionalità di preparazione automatica a livello di account per tutti gli indirizzi IP.

Se disabiliti la funzione di preparazione automatica, tutti gli IP dedicati successivamente noleggiati verranno aggiunti all'account con lo stato di preparazione Complete (Completato), che li rende disponibili per l'uso senza essere stati preparati. Ciò significa che è necessario assicurarsi che questi IP siano adeguatamente preparati prima dell'uso finalizzato all'invio regolare. Tutti gli IP la cui fase di preparazione era in corso al momento in cui è stata disabilitata la funzione di preparazione automatica non verranno modificati.

> **Important**
>
> Se disabiliti la caratteristica di preparazione automatica, diventi responsabile della preparazione dei tuoi indirizzi IP dedicati. Se invii e-mail da indirizzi che non sono stati preparati, potresti registrare frequenze di recapito insoddisfacenti.

Disabilitazione (o riabilitazione) della funzione di preparazione automatica per tutti gli IP dedicati (standard) nell'account in uso

1. Accedi alla AWS Management Console e apri la console Amazon SES all'indirizzo https://console.aws.amazon.com/ses/.
2. Nel riquadro di navigazione a sinistra, scegli Dedicated IPs (IP dedicati).
3. Seleziona la scheda Standard IP pools (Pool IP standard) nella pagina Dedicated IPs (IP dedicati).
4. Scegli Disable auto warm-up (Disabilita preparazione automatica) nel pannello Standard overview (Panoramica standard) per disabilitare la preparazione automatica oppure scegli Enable auto warm-up (Abilita preparazione automatica) per riabilitarla.

Preparazione manuale degli IP dedicati (standard)

È possibile aumentare o diminuire manualmente il volume di invio corrente degli IP dedicati (standard) modificando la relativa percentuale di preparazione, terminare il processo di preparazione

prematuramente e impostare il volume di invio corrente sullo 0% e riavviare il processo di preparazione.

Preparazione manuale di IP dedicati (standard)

1. Accedi alla AWS Management Console e apri la console Amazon SES all'indirizzo https://console.aws.amazon.com/ses/.
2. Nel riquadro di navigazione a sinistra, scegli Dedicated IPs (IP dedicati).
3. Seleziona la scheda Standard IP pools (Pool IP standard) nella pagina Dedicated IPs (IP dedicati).
4. Nel pannello All Standard dedicated IPs (Tutti gli IP dedicati standard), seleziona un indirizzo IP e scegli Edit warm up (Modifica preparazione, quindi seleziona una delle seguenti opzioni:

   a. Edit percentage (Modifica percentuale): inserisci un valore nel campo Warm-up percentage (Percentuale di preparazione) per aumentare o diminuire il volume di invio corrente dell'IP modificando la percentuale di riscaldamento, quindi scegli Save changes (Salva modifiche).

      Nella colonna Warm-up status (Stato preparazione) sarà riportato `In progress`, mentre nella colonna Warm-up percentage (Percentuale di preparazione) è indicato il valore inserito.

   b. Mark as Complete (Contrassegna come completata): facendo riferimento alla finestra di dialogo Mark warm-up as Complete?(Contrassegnare la preparazione come completata?), conferma di aver compreso le implicazioni dell'interruzione prematura del processo di preparazione automatica, quindi scegli Mark as Complete (Contrassegna come completata).

      Nella colonna Warm-up status (Stato preparazione) sarà riportato `Complete`, mentre nella colonna Warm-up percentage (Percentuale di preparazione) è indicato `100%`.

   c. Reset percentage (Reimposta percentuale): facendo riferimento alla finestra di dialogo Reset warm-up percentage? (Reimpostare la percentuale di preparazione?), conferma di aver impostato il volume di invio corrente dell'IP su 0%, do riavviare il processo di preparazione automatica o di impostare la percentuale di preparazione manualmente, quindi scegli Reset (Reimposta).

      Nella colonna Warm-up status (Stato preparazione) sarà riportato `In progress`, mentre nella colonna Warm-up percentage (Percentuale di preparazione) è indicato `0%`.

Creazione di pool IP dedicati standard per IP dedicati (standard)

Se hai acquistato diversi indirizzi IP dedicati (standard) per l'uso con Amazon SES, puoi creare gruppi di tali indirizzi denominati pool di IP dedicati. Il raggruppamento di IP dedicati (standard) in un pool ne semplifica la gestione. Uno scenario comune consiste nella creazione di un pool per l'invio di comunicazioni di marketing e di un altro per l'invio di e-mail transazionali. La tua reputazione di mittente per le e-mail transazionali è quindi isolata da quella delle e-mail di marketing. In questo scenario, se una campagna di marketing genera un numero elevato di reclami, la consegna delle tue e-mail transazionali non viene compromessa.

Questa sezione contiene le procedure per la creazione di pool di IP dedicati.

> **Note**
>
> Puoi anche creare set di configurazione che utilizzino un pool di indirizzi IP condivisi da tutti i clienti SES. Il pool di IP condivisi è utile in situazioni in cui è necessario inviare e-mail non compatibili con i comportamenti di invio consueti. Per informazioni sull'utilizzo del pool di IP condivisi con un set di configurazione, consulta Assegnazione di pool di IP in Amazon SES.

Creazione di un pool di IP dedicati per IP dedicati (standard) tramite la console SES

1. Accedi alla AWS Management Console e apri la console Amazon SES all'indirizzo https://console.aws.amazon.com/ses/.
2. Nel riquadro di navigazione a sinistra, scegli Dedicated IPs (IP dedicati).

   > **Note**
   >
   > Se al momento non disponi di IP dedicati (standard) nell'account, viene visualizzata la pagina di onboarding Dedicated IPs (IP dedicati) da cui potrai acquistare IP dedicati (standard). Per ulteriori informazioni, consulta the section called “Richiesta di IP dedicati (standard)”.

3. Seleziona la scheda Standard IP pools (Pool IP standard) nella pagina Dedicated IPs (IP dedicati).
4. Nel pannello All Dedicated IP (standard) pools (Tutti i pool IP dedicati (standard)), scegli Create Standard IP pool (Crea pool IP standard).

Viene aperta la pagina Create IP Pool (Crea pool IP).

5. Nel pannello Pool details (Dettagli pool):

   a. Scegli Standard (self managed) (Standard (autogestito)) nel campo Scaling mode (Modalità dimensionamento).

   b. Inserisci un nome del pool di IP nel campo IP pool name (Nome pool IP).

   > **Note**
   >
   > Il nome del pool di IP deve essere univoco e non può essere un duplicato del nome di un pool di IP gestiti nell'account.

   c. (Facoltativo) Se sono presenti indirizzi IP dedicati standard che desideri aggiungere a questo pool di IP, selezionali nell'elenco a discesa nel campo Dedicated IP addresses (Indirizzi IP dedicati).

   > **Note**
   >
   > Se selezioni un indirizzo IP già associato a un pool di IP, verrà associato solo a tale pool.

6. (Facoltativo) È possibile associare questo pool di IP a un set di configurazione selezionandone uno nell'elenco a discesa nel campo Configuration sets (Set di configurazione).

   > **Note**
   >
   > - Se si seleziona un set di configurazione già associato a un pool di IP, ora verrà associato solo a tale pool.
   > - Per aggiungere o rimuovere i set di configurazione associati dopo la creazione di questo pool di IP, modifica il parametro Sending IP pool (Pool di IP di invio) del set di configurazione.
   > - Se non hai ancora creato set di configurazione, consulta Set di configurazione.

7. (Facoltativo) Puoi aggiungere uno o più tag al pool di IP includendo una chiave di tag e un valore facoltativo per la chiave.

a. Scegli Add new tag (Aggiungi nuovo tag) e immetti il valore per Key (Chiave). È possibile aggiungere un valore facoltativo al tag in Value (Valore).

b. Per aggiungere il tag, seleziona Save changes (Salva modifiche).

   Puoi aggiungere fino a 50 tag. Puoi rimuovere eventuali righe esistenti scegliendo Remove (Rimuovi).

8. Seleziona Create Pool (Crea pool).

> **Note**
>
> Dopo essere stato creato, un pool di IP standard può essere convertito in un pool di IP gestiti. Per informazioni, consultare Creazione di un pool di IP gestiti.

Indirizzi IP dedicati (gestiti) per Amazon SES

Gli indirizzi IP dedicati (gestiti) sono una funzionalità di Amazon SES che imposta e gestisce automaticamente gli indirizzi IP dedicati in modo da poter iniziare a utilizzare in modo semplice e veloce gli indirizzi IP dedicati gestiti da SES. Questo garantisce che gli indirizzi IP dedicati vengano utilizzati in modo efficiente e ottimale per le modalità di invio di e-mail in uso.

Per abilitare gli IP dedicati (gestiti) nell'account, ti basta creare un pool di IP gestiti e SES si occuperà di tutto il resto. SES stabilirà il numero di IP dedicati necessari in base ai tuoi schemi di invio, li creerà per te e quindi ne gestirà il ridimensionamento in base alle tue esigenze di invio.

Una volta abilitati, puoi utilizzare gli IP dedicati (gestiti) nell'invio di e-mail associando il pool di IP gestiti a un set di configurazione e quindi specificando tale set di configurazione durante l'invio di e-mail. Il set di configurazione può essere applicato anche a un'identità di invio utilizzando un set di configurazione predefinito.

Vantaggi e caratteristiche degli IP dedicati (gestiti)

Gli indirizzi IP dedicati che crei con IP dedicati (gestiti) automatizzano le attività di gestione per garantire che gli indirizzi IP dedicati vengano utilizzati in modo ottimale per la modalità di invio di e-mail in uso:

- Onboarding semplice: per iniziare a utilizzare IP dedicati (gestiti), è possibile creare un pool di IP gestiti direttamente dalla console SES. Gli indirizzi IP dedicati vengono assegnati automaticamente

al pool. Puoi iniziare a inviare con il pool IP gestito senza dover aprire un caso di richiesta tramite il AWS Support Center.

- Scalabilità automatica per ISP: non è necessario monitorare o ridimensionare manualmente i pool IP dedicati perché il pool IP gestito si ridimensiona automaticamente in base all'utilizzo. Prende in considerazione anche le policy specifiche del fornitore di servizi Internet (ISP). Ad esempio, se SES rileva che un fornitore di servizi Internet (ISP) supporta una quota di invio giornaliera bassa, il pool si ridimensiona per distribuire meglio il traffico verso tale fornitore di servizi Internet (ISP) su più indirizzi IP.
- Preparazione intelligente: gli IP dedicati (gestiti) iniziano a inviare posta ai fornitori di servizi Internet (ISP) in base alla loro capacità, ovvero in base a loro livello di preparazione. Tengono automaticamente traccia del livello di preparazione per ogni singolo fornitore di servizi Internet (ISP). Inoltre, la funzionalità IP dedicati (gestiti) fornisce informazioni sulla tua reputazione a una tariffa giornaliera effettiva con i migliori ISP sotto forma di CloudWatch metriche Amazon e dashboard integrate.
  - Preparazione per fornitore di servizi Internet (ISP): SES tiene traccia della reputazione di ogni IP nel pool di IP gestiti per ciascun fornitore di servizi Internet (ISP). Ad esempio, se hai inviato tutto il traffico a Gmail, gli indirizzi IP vengono considerati preparati solo per Gmail e non preparati per gli altri fornitori di servizi Internet (ISP). Se modifichi il modello di traffico aumentando le email inviate a Hotmail, SES aumenta lentamente il traffico per Hotmail, poiché gli indirizzi IP non sono ancora preparati.
  - Riscaldamento adattivo e transizione alla piscina condivisa: la regolazione del riscaldamento è adattiva e tiene conto degli schemi di invio effettivi. Quando il volume di invio a un fornitore di servizi Internet (ISP) diminuisce, anche la percentuale di preparazione diminuisce per tale fornitore. Nella fase iniziale del riscaldamento, qualsiasi invio eccessivo in base all'attuale livello di riscaldamento viene inviato tramite gli indirizzi IP condivisi con altri utenti di Amazon SES, il pool condiviso SES. Nelle fasi successive del preparazione, qualsiasi invio eccessivo viene rallentato in modo proattivo e riprovato in seguito.

> **Important**
>
> Sebbene gli IP dedicati (gestiti) riscaldino automaticamente gli indirizzi IP dedicati, parte di questo processo automatico consiste nel lavorare in modo interattivo con il pool IP condiviso di SES.
>
> - Se la velocità di invio è troppo aggressiva per i nuovi IP dedicati durante la fase di aggiornamento, SES trasferirà automaticamente parte dell'invio nel pool di IP condivisi di SES per proteggere la reputazione dei nuovi IP dedicati.

- Anche dopo che i tuoi nuovi IP dedicati si saranno completamente riscaldati, non è garantito che tutti i tuoi invii vengano ricevuti il 100% delle volte. Ad esempio, se la velocità di invio aumenta improvvisamente e gli IP dedicati (gestiti) determinano la necessità di allocare un indirizzo IP dedicato aggiuntivo, avvieranno il processo di riscaldamento che include l'utilizzo del pool condiviso. Allo stesso modo, se la tua velocità di invio scende improvvisamente a un livello molto basso, tutte le tue spedizioni potrebbero passare al pool di IP condivisi di SES, vedi. the section called “Importanza della preparazione”

- Richiesta e rinuncia automatiche di indirizzi IP dedicati: non è necessario richiedere o rinunciare a indirizzi IP dedicati gestiti tramite il AWS Support Center, come è richiesto quando si utilizzano IP dedicati (standard). Quando effettui l'onboarding con IP dedicati (gestiti) direttamente dalla console SES, dall'interfaccia della riga di comando o dall'API, vengono assegnati automaticamente indirizzi IP dedicati e viene addebitata una tariffa in base al volume di messaggi inviati. Quando elimini un pool di IP creato da IP dedicati (gestiti) o disattivi gli IP dedicati (gestiti), gli indirizzi IP assegnati vengono automaticamente rilasciati e gli addebiti cessano immediatamente.
  - Ottenere il primo indirizzo IP dedicato: la funzionalità IP dedicati (gestiti) assegnerà automaticamente il primo indirizzo IP dedicato quando il volume di invio raggiunge centinaia di e-mail nell'arco di pochi giorni. Ciò garantisce che l'IP da cui si esegue l'invio possa creare una reputazione di invio e migliorare l'efficienza del recapito. Se non si prevede che il volume di invio raggiunga questo livello, è opportuno utilizzare indirizzi IP condivisi. Consulta la tabella di confronto in Indirizzi IP dedicati per esaminare il tipo di indirizzi IP più adatto alla modalità di invio delle e-mail in uso.

Perché è importante una corretta preparazione IP

Per garantire che l'e-mail venga recapitata tramite l'indirizzo IP dedicato, è necessario che disponga di una buona reputazione presso l'ISP ricevente. Gli ISP accetteno solo un piccolo volume di e-mail da un IP che non riconoscono. La prima volta che viene assegnato, un IP è nuovo e non viene riconosciuto dall'ISP ricevente perché non ha una reputazione associata. Affinché venga stabilita una reputazione, un IP deve gradualmente rafforzare la fiducia con l'ISP ricevente. Questo processo graduale di costruzione della fiducia viene definito preparazione. Subito dopo l'assegnazione di un IP da parte di IP dedicati (gestiti), viene avviato il processo di preparazione intelligente.

Con le funzionalità Preparazione per ISP e Preparazione adattiva di IP dedicati (gestiti), la continuità aziendale viene mantenuta per tutto il ciclo di preparazione assicurando che le e-mail vengano

recapitate. Una volta completata la fase di preparazione, l'eventuale capacità in eccesso viene aggiunta alla coda e inviata solo attraverso il pool di IP dedicati. Tuttavia, se disponi di un indirizzo IP dedicato e il volume di invio scende al di sotto del volume minimo richiesto per mantenere la reputazione IP, gli IP dedicati (gestiti) potrebbero rimuovere l'IP dedicato e l'invio verrà instradato attraverso il pool di IP condivisi di SES.

> **Note**
>
> Se si inviano piccoli volumi di e-mail (meno di qualche centinaio al giorno nell'arco di pochi giorni), è più vantaggioso inviare tramite il pool di IP condivisi SES. Verifica se IP dedicati (gestiti) è adatto alla modalità corrente di invio della posta esaminando la tabella di confronto in Indirizzi IP dedicati.

Creazione di un pool di IP gestiti per abilitare gli IP dedicati (gestiti)

Per abilitare gli IP dedicati (gestiti) devi prima creare un pool di IP gestiti. Dopo aver creato un pool gestito, la funzionalità determina il numero di IP dedicati necessari in base ai modelli di invio e si ridimensiona dinamicamente in base alle esigenze.

Per utilizzare il pool gestito per inviare e-mail, è necessario associare il pool gestito a un set di configurazione e quindi specificare tale set al momento di inviare l'e-mail. Il set di configurazione può essere applicato anche a un'identità di invio utilizzando un set di configurazione predefinito.

Esistono due modi per creare un pool di IP gestiti:

- Creazione di un nuovo pool.
- Conversione di un pool esistente da standard a gestito.

Nelle procedure che seguono sono fornite istruzioni per entrambi i metodi.

Creazione o conversione di un pool di IP gestiti tramite la console SES

1. Accedi AWS Management Console e apri la console Amazon SES all'indirizzo https://console.aws.amazon.com/ses/.
2. Nel riquadro di navigazione a sinistra, scegli Dedicated IPs (IP dedicati).
3. A seconda che tu voglia creare un nuovo pool di IP gestiti o convertire un pool di IP dedicati standard in uno gestito, segui le relative istruzioni:

Create new pool

Per creare un nuovo pool di IP gestiti

1. Esegui una di queste operazioni:

   a. Se nel tuo account non sono già presenti IP dedicati:

      - Viene aperta la pagina di onboarding Dedicated IPs (IP dedicati). Nel pannello di Dedicated IPs (managed) overview (Panoramica degli IP dedicati (gestiti)), scegli Enable dedicated IPs (Abilita IP dedicati).

        Viene aperta la pagina Create IP Pool (Crea pool IP).

   b. Se nel tuo account sono già presenti IP dedicati:

      i. Seleziona la scheda Managed IP pools (Pool IP gestiti) nella pagina Dedicated IPs (IP dedicati).

      ii. Nel pannello All Dedicated IP (managed) pools (Tutti i pool IP dedicati (gestiti)), scegli Create Managed IP pool (Crea pool IP gestiti).

      Viene aperta la pagina Create IP Pool (Crea pool IP).

2. Nel pannello Pool details (Dettagli pool):

   a. Scegli Managed (auto managed) (Gestito [autogestione]) nel campo Scaling mode (Modalità dimensionamento).

   b. Inserisci un nome del pool gestito nel campo IP pool name (Nome pool IP).

   > **Note**
   >
   > - Il nome del pool di IP deve essere univoco. Non può essere il duplicato di un nome di pool di IP dedicati standard nell'account in uso.
   > - Non puoi avere più di 50 pool di IP dedicati per Regione AWS nel tuo account, inclusi pool di IP gestiti e pool di IP standard.

3. (Facoltativo) È possibile associare questo pool di IP gestiti a un set di configurazione scegliendone uno nell'elenco a discesa nel campo Configuration sets (Set di configurazione).

> **Note**
>
> - Se si sceglie un set di configurazione già associato a un pool di IP, questo verrà associato a tale pool gestito e non sarà più associato al pool precedente.
> - Per aggiungere o rimuovere i set di configurazione associati dopo la creazione di questo pool gestito, modifica il parametro Sending IP pool (Pool di IP di invio) del set di configurazione nel pannello General details (Dettagli generali).
> - Se non hai ancora creato set di configurazione, consulta Set di configurazione.

4. (Opzionale) Puoi aggiungere uno o più tag al pool di IP includendo una chiave di tag e un valore facoltativo per la chiave.

   a. Scegli Add new tag (Aggiungi nuovo tag) e immetti il valore per Key (Chiave). È possibile aggiungere un valore facoltativo al tag in Value (Valore). Puoi aggiungere fino 50 tag. In caso di errore, scegli Remove (Elimina).

   b. Per aggiungere i tag, seleziona Save changes (Salva modifiche).

   Dopo aver creato il pool, potrai aggiungere, rimuovere o modificare i tag selezionando il pool gestito e scegliendo Edit (Modifica).

5. Seleziona Create Pool (Crea pool).

> **Note**
>
> - Dopo essere stato creato, un pool di IP gestiti non può essere convertito in un pool di IP standard.
> - Quando utilizzi IP dedicati (gestiti), non puoi avere più di 10.000 identità di invio (domini e indirizzi e-mail, in qualsiasi combinazione) per Regione AWS account.

Convert standard to managed

Per convertire un pool di IP dedicati standard in un pool di IP gestiti

1. Seleziona la scheda Standard IP pools (Pool IP standard) nella pagina Dedicated IPs (IP dedicati).

2. Nel pannello Tutti i pool di IP dedicati (standard), seleziona la casella di controllo del pool di IP dedicati che desideri convertire da standard a gestito.
3. Scegli Converti in pool gestito: leggi la finestra di dialogo Converti in pool di IP gestiti per confermare di aver compreso le condizioni di conversione del pool di IP dedicati standard in uno gestito.

> **Note**
>
> Prima di convertire il pool di IP dedicati da standard a gestito, tieni presente quanto segue:
>
> 1. Tutti gli attuali IP dedicati (standard) verranno spostati nel pool gestito.
> 2. Se al momento stai noleggiando troppi IP dedicati (standard) per il tuo volume di invio, gli IP dedicati (gestiti) rimuoveranno gli IP ridondanti.
> 3. Se uno degli IP dedicati (standard) fa parte di un elenco di autorizzazioni per altre applicazioni, non dovresti trasferirli nel pool gestito poiché verranno rimossi se diventano ridondanti. Fai riferimento al punto 2.
> 4. Non ti verrà più addebitato un costo per IP, ma ti verrà addebitato un costo in base al volume inviato tramite il pool gestito. Consulta Prezzi di Amazon SES.

4. Se accetti le condizioni indicate, scegli Conferma: viene visualizzato un banner che conferma che il pool di IP dedicati standard è stato convertito in un pool gestito.

> **Note**
>
> Tutti i set di configurazione o i tag che avevi associato al pool standard prima della conversione verranno ora associati al pool gestito, fornendo una transizione senza interruzioni per qualsiasi invio di e-mail mediante il set di configurazione.

Puoi anche utilizzare la pubblicazione degli eventi per tenere traccia delle prestazioni di invio del pool gestito. Per ulteriori informazioni, consulta the section called “Monitoraggio dell'invio di e-mail utilizzando la pubblicazione di eventi”.

Visualizzazione dell'invio e della capacità gestiti del pool di IP gestiti tramite la console Amazon SES

Per i pool di IP gestiti creati, la console SES offre un modo semplice per osservare come vengono utilizzati per l'invio di e-mail tramite schede e grafici di serie temporali che mostrano le metriche di invio e l'utilizzo e la capacità dell'ISP.

Visualizzazione dell'invio e della capacità gestiti del pool di IP gestiti tramite la console Amazon SES

1. Accedi AWS Management Console e apri la console Amazon SES all'indirizzo https://console.aws.amazon.com/ses/.
2. Nel riquadro di navigazione a sinistra, scegli Dedicated IPs (IP dedicati).
3. Seleziona la scheda Managed IP pools (Pool IP gestiti) nella pagina Dedicated IPs (IP dedicati).
4. A seconda che desideri visualizzare i parametri di invio e capacità nella console Amazon SES o nella CloudWatch console Amazon, segui le rispettive istruzioni:

   Amazon SES console

   Visualizzazione delle metriche di invio e capacità nella console Amazon SES

   1. Nella tabella Tutti i pool di IP dedicati (gestiti), seleziona il nome di un pool di IP gestiti elencato nella colonna Pool di IP per visualizzarne i dettagli.

      La pagina dei dettagli del pool di IP selezionato si apre con le seguenti schede e grafici delle serie temporali:

      a. Schede:

         - Stato di invio: indica se il volume e la frequenza di invio sono sufficienti per utilizzare gli IP dedicati visualizzando uno dei due stati:
           - Volume insufficiente: il volume di invio è troppo basso.
           - Invio tramite IP dedicati: nel pool gestito vengono utilizzati uno o più IP dedicati.
         - Volume di invio IP dedicati gestiti: il volume di e-mail inviate tramite IP dedicati nel pool gestito negli ultimi 7 giorni.
         - Frequenza di invio di IP dedicati gestiti: percentuale di e-mail inviate che sono state consegnate correttamente tramite IP dedicati nel pool gestito negli ultimi 7 giorni.

b. Grafici:

- Volume inviato: il volume di e-mail inviate negli ultimi 7 giorni tramite IP dedicati gestiti rispetto agli IP condivisi.
- Percentuale del volume inviato: la percentuale di e-mail inviate negli ultimi 7 giorni tramite IP dedicati gestiti rispetto agli IP condivisi.
- Capacità ISP: mostra la quantità di e-mail inviate tramite IP dedicati nel pool gestito per i 10 ISP più utilizzati e la loro capacità disponibile durante l'invio:
  - Invii per ISP (barre rosse): il volume di e-mail che hai inviato nelle ultime 24 ore tramite l'ISP selezionato.
  - Capacità dell'ISP (linea blu): la capacità disponibile dell'ISP selezionato nelle ultime 24 ore.

2. Per filtrare un ISP specifico in base al grafico della Capacità dell'ISP, scegli la casella di riepilogo ISP e seleziona un ISP: il grafico verrà aggiornato con le metriche per l'ISP selezionato. (Se non applichi filtri su un ISP, per impostazione predefinita viene visualizzato Gmail).

Amazon CloudWatch console

Per visualizzare i parametri di invio e capacità nella console Amazon CloudWatch

- Nella tabella Tutti i pool con IP dedicati (gestiti), seleziona il <pool_name>link Visualizza CloudWatch metriche nella colonna delle CloudWatchmetriche per visualizzarne i dettagli.

  La pagina del pool di IP selezionato si apre nella CloudWatch console e mostra le seguenti metriche:

  - Invio: il volume di e-mail inviato tramite IP dedicati gestiti e IP condivisi.
  - ApproximateDedicatedSendingPercentage— Indica la percentuale approssimativa di traffico erogato tramite un IP dedicato.
  - SentLast24 ore: il volume di e-mail che hai inviato nelle ultime 24 ore tramite l'ISP selezionato. (Etichettato come Invii per ISP nella console SES.)
  - Available24 HourSend: la capacità disponibile dell'ISP selezionato nelle ultime 24 ore. (Etichettato come Capacità per ISP nella console SES.)

Eliminazione di un pool di IP gestiti e disattivazione degli IP dedicati (gestiti)

L'eliminazione di un pool di IP gestiti comporta il rilascio automatico di tutti gli indirizzi IP ad esso allocati. Se disponi di un solo pool di IP gestiti e lo elimini, oppure elimini l'ultimo pool di IP gestiti rimasto, disattiverai la funzionalità di IP dedicati (gestiti) e gli addebiti cesseranno immediatamente.

Eliminazione di un pool di IP gestiti tramite la console SES

1. Accedi AWS Management Console e apri la console Amazon SES all'indirizzo https://console.aws.amazon.com/ses/.
2. Nel riquadro di navigazione a sinistra, scegli Dedicated IPs (IP dedicati).
3. Seleziona la scheda Managed IP pools (Pool IP gestiti) nella pagina Dedicated IPs (IP dedicati).
4. Nella tabella All Dedicated IP (managed) pools (Tutti i pool di IP dedicati (gestiti)), seleziona il pulsante di opzione accanto al nome del pool IP (IP pool) gestito che desideri rimuovere e scegli Delete (Elimina).
5. Nella finestra popup, avrai la possibilità di confermare la tua scelta selezionando Delete (Elimina) o Cancel (Annulla) per mantenere il pool gestito.

> **Note**
>
> Se disponi di un solo pool gestito o stai rimuovendo l'ultimo, la finestra popup ti ricorderà che l'eliminazione del pool gestito rimanente comporta la disattivazione della funzionalità di IP dedicati (gestiti) e che non ti verrà più addebitato alcun costo. Ti verrà richiesto di immettere *`Disable`* nel campo di conferma prima di poter scegliere Delete (Elimina).

Utilizzo dei propri indirizzi IP per inviare e-mail con Amazon SES

Amazon SES include una caratteristica denominata Bring Your Own IP (BYOIP), che consente di utilizzare i propri indirizzi IP per inviare e-mail con Amazon SES. Se utilizzi già un intervallo di indirizzi IP per inviare e-mail, puoi richiedere che il tuo intervallo IP sia disponibile per l'invio di email con Amazon SES.

> **Note**
>
> La funzionalità BYOIP è disponibile solo per gli indirizzi IP dedicati configurati manualmente e non può essere utilizzata con IP dedicati (gestiti).

BYOIP è utile, ad esempio, quando hai sviluppato una reputazione IP positiva utilizzando un sistema di invio e-mail interno, ma desideri eseguire la migrazione ad Amazon SES. Utilizzando BYOIP, puoi iniziare a inviare e-mail con Amazon SES immediatamente, senza dover ristabilire la reputazione dei tuoi indirizzi IP.

Requisiti

Per utilizzare BYOIP, l'intervallo di indirizzi IP deve soddisfare i seguenti requisiti:

- L'intervallo di indirizzi deve essere registrato nel tuo registro Internet regionale (RIR), come American Registry for Internet Numbers (ARIN), Réseaux IP Européens Network Coordination Centre (RIPE NCC) o Asia-Pacific Network Information Centre (APNIC). L'intervallo di indirizzi deve essere registrato in un'entità aziendale o istituzionale e non può essere registrato per una persona.
- Devi inoltre provare di essere il proprietario dell'intervallo di indirizzi tramite un messaggio di autorizzazione firmato.
- Gli indirizzi nell'intervallo di indirizzi IP devono avere una cronologia pulita. È opportuno esaminare la reputazione dell'intervallo di indirizzi IP e riservarsi il diritto di rifiutare un intervallo di indirizzi IP se contiene indirizzi IP con scarsa reputazione o associati a un comportamento dannoso.
- L'intervallo di indirizzi IP non può includere intervalli di indirizzi IP inseriti in un altro Servizio AWS per BYOIP, come Amazon EC2.

Considerazioni

Esistono diversi fattori da considerare prima di richiedere il trasferimento degli intervalli IP ad Amazon SES:

- La più ampia gamma di indirizzi che puoi specificare è /24. In altre parole, se trasferisci l'intervallo IP 203.0.113.0/24 al tuo account Amazon SES, puoi inviare da un totale di 256 indirizzi, che vanno da 203.0.113.0 a 203.0.113.255. Devi trasferire l'intero intervallo; Amazon SES attualmente non consente di trasferire singoli indirizzi IP.
- Se utilizzi BYOIP per un intervallo specifico di indirizzi IP, puoi accedere all'intervallo solo da una singola Regione AWS.
- Puoi portare cinque intervalli di indirizzi per Regione nel tuo Account AWS.
- Se utilizzi i tuoi indirizzi IP, non puoi usare gli indirizzi del pool di indirizzi IP condivisi di Amazon SES. Se è necessario utilizzare questi indirizzi IP condivisi, puoi utilizzare Amazon SES in un'altra Regione AWS o creare un nuovo Account AWS.

- È previsto un addebito mensile per ogni indirizzo IP utilizzato con BYOIP. Per ulteriori informazioni, consulta la pagina dei Prezzi di Amazon SES.

Utilizzo dei propri indirizzi IP con Amazon SES

Per evitare che i nostri sistemi vengano utilizzati per l'invio di contenuti indesiderati o dannosi, ogni richiesta BYOIP dovrà essere analizzata attentamente da parte nostra.

Se desideri utilizzare il tuo intervallo IP con Amazon SES invia le seguenti informazioni a ses-byoip-request@amazon.com:

- ID dell'account AWS;
- Regione AWS in cui desideri utilizzare l'intervallo IP, ad esempio ap-south-1.
- descrizione del caso d'uso;
- intervallo IP con cui desideri utilizzare Amazon SES;
- nome del registro Internet con cui è registrato l'intervallo.

Risponderemo alla tua richiesta entro 48 ore lavorative. Nelle nostre comunicazioni, potremmo richiedere ulteriori informazioni, inclusi documenti che dimostrino la tua proprietà dell'intervallo IP.

Virtual Deliverability Manager per Amazon SES

L'efficienza del recapito, ovvero la garanzia che le tue e-mail arrivino nella posta in arrivo dei destinatari anziché nelle cartelle dello spam o della posta indesiderata, è fondamentale per una strategia ottimale a livello di e-mail.

Virtual Deliverability Manager è una funzionalità di Amazon SES che aiuta a migliorare questo aspetto, ad esempio aumentando l'efficienza del recapito nella casella di posta in arrivo e le conversioni delle e-mail, fornendo informazioni sui dati di invio e recapito e offrendo consigli su come risolvere i problemi che influiscono negativamente sul tasso di successo dei recapiti e sulla tua reputazione.

Importanza dell'efficienza del recapito nella casella di posta in arrivo e della reputazione del mittente

L'efficienza del recapito nella casella di posta in arrivo è essenziale per le conversioni e-mail (ovvero il momento in cui un destinatario esegue un'azione dopo aver aperto un'e-mail): i clienti che non ricevono i tuoi messaggi non saranno in grado di vederli e tanto meno di interagire con loro.

A livello di esperienza del cliente, la reputazione dell'invio è un fattore chiave per l'efficienza del recapito nella casella di posta in arrivo: determina infatti l'arrivo ai destinatari di messaggi indesiderati oppure il blocco o lo smistamento di messaggi necessari alle cartelle di posta indesiderata prima che possano arrivare nelle caselle di posta dei destinatari.

Come Virtual Deliverability Manager può contribuire a migliorare l'efficienza del recapito e la reputazione

Virtual Deliverability Manager aiuta a migliorare l'efficienza di recapito e la reputazione con una dashboard che offre viste generali e dettagliate del programma e-mail del tuo account, utili per concentrarti su eventuali aree problematiche, nonché con un advisor in grado di fornire soluzioni per risolvere i problemi infrastrutturali che influiscono negativamente sull'efficienza del recapito e sulla reputazione delle tue e-mail.

- Dashboard: fornisce informazioni sui dati relativi all'efficienza del recapito, con attenzione su account, ISP, identità di invio e livelli di set di configurazione. Tutto questo consente di individuare rapidamente le aree e le tendenze problematiche e di identificare eventuali difficoltà prima che si trasformino in problemi di consegna più seri, come rifiuti temporanei (rinvii) o blocchi. Queste informazioni sono anche utili per migliorare la reputazione del mittente grazie al calcolo di orari e date ideali per sviluppare il coinvolgimento dei clienti e le conversioni per le campagne e-mail.

- Advisor: fornisce consigli per migliorare l'invio delle e-mail segnalando i problemi di configurazione che influiscono negativamente sull'efficienza di recapito e sulla reputazione delle e-mail. L'advisor consiglierà soluzioni per risolvere problemi specifici nell'infrastruttura del dominio di invio, dello spazio IP e dei record di autenticazione, ad esempio se i record SPF, DMARC o DKIM sono assenti o se la chiave DKIM è troppo breve.

Iniziare a utilizzare Virtual Deliverability Manager

Potrai iniziare a usare Virtual Deliverability Manager seguendo una procedura guidata di onboarding nella console Amazon SES, che ti guiderà nei passaggi necessari per abilitare Virtual Deliverability Manager per il tuo account. Per informazioni, consulta the section called “Nozioni di base”.

Argomenti

Iniziare a utilizzare Virtual Deliverability Manager

Per iniziare a utilizzare Virtual Deliverability Manager con il tuo account, devi abilitarlo seguendo la procedura guidata di onboarding nella console Amazon SES, dove potrai configurare il monitoraggio del coinvolgimento e la consegna condivisa ottimizzata. Virtual Deliverability Manager utilizza il monitoraggio del coinvolgimento e la consegna condivisa ottimizzata per monitorare gli invii e aiutarti a migliorare l'efficienza del recapito e la tua reputazione.

- Monitoraggio del coinvolgimento: la capacità di monitorare il comportamento di coinvolgimento dei destinatari tramite eventi di apertura e clic con un pixel di tracciamento all'interno di un link con wrapping. Quando viene attivato, il pixel di tracciamento fornisce un timestamp dell'apertura del messaggio e indica su quali link ha fatto clic il destinatario. Attivando questa opzione, i tuoi URL e link vengono modificati in modo da includere i wrapper di tracciamento del coinvolgimento di Amazon SES.
- Consegna condivisa ottimizzata: sceglie automaticamente l'IP ottimale da utilizzare per l'invio di e-mail, migliorando la consegna finale dei messaggi ai destinatari delle e-mail. Questo non vale per gli indirizzi IP dedicati.

Il monitoraggio del coinvolgimento e la consegna condivisa ottimizzata sono entrambi attivati per impostazione predefinita nella procedura guidata di onboarding, ma hai la possibilità di disattivarli. Ti consigliamo vivamente di mantenere abilitate entrambe le funzionalità per ottenere il massimo dal Gestore virtuale della deliverability delle email.

Iniziare a utilizzare Virtual Deliverability Manager tramite la console Amazon SES

La procedura seguente illustra le nozioni di base relative a Virtual Deliverability Manager tramite la console Amazon SES.

Per iniziare a utilizzare Virtual Deliverability Manager tramite la console Amazon SES

1. Accedi alla AWS Management Console e apri la console Amazon SES all'indirizzo https://console.aws.amazon.com/ses/.
2. Nel riquadro di navigazione a sinistra, scegli Virtual Deliverability Manager.
3. Scegli uno dei pulsanti Get started with Virtual Deliverability Manager (Inizia a usare Virtual Deliverability Manager) nella pagina Virtual Deliverability Manager overview (Panoramica di Virtual Deliverability Manager).
4. Nella pagina Select Engagement tracking (Seleziona monitoraggio del coinvolgimento), accetta l'impostazione predefinita o scegli Turn off engagement tracking (Disattiva il monitoraggio del coinvolgimento), quindi scegli Next (Successivo).

   > **Note**
   >
   > Attivando il monitoraggio del coinvolgimento, i tuoi URL e link vengono modificati in modo da includere i wrapper di tracciamento del coinvolgimento di Amazon SES.

5. Nella pagina Select Optimized shared delivery (Seleziona Consegna condivisa ottimizzata), accetta l'impostazione predefinita o scegli Turn off optimized shared delivery (Disattiva la consegna condivisa ottimizzata), quindi scegli Next (Successivo).

   > **Important**
   >
   > La consegna condivisa ottimizzata potrebbe comportare ritardi nell'invio delle e-mail, volti a proteggere la tua reputazione di invio. Se hai un carico di lavoro critico che deve essere inviato senza ritardi, ti consigliamo di non abilitare questa impostazione. Utilizza

invece i set di configurazione per l'invio e abilita la consegna condivisa ottimizzata solo per quei set di configurazione per cui sono ammissibili ritardi.

6. Controlla le tue scelte per il monitoraggio del coinvolgimento e la consegna condivisa ottimizzata nella pagina Review and enable (Valuta e abilita). Scegli Previous (Precedente) se desideri tornare indietro e apportare modifiche; altrimenti, scegli Enable Virtual Deliverability Manager (Abilita Virtual Deliverability Manager).

   Viene aperta la pagina Virtual Deliverability Manager settings (Impostazioni di Virtual Deliverability Manager). Il pannello Subscription overview (Panoramica delle sottoscrizioni) indica lo stato di Virtual Deliverability Manager, mentre il pannello Additional settings (Impostazioni aggiuntive) mostra lo stato delle funzionalità Engagement tracking (Monitoraggio del coinvolgimento) e Optimized shared delivery (Consegna condivisa ottimizzata).

Dopo aver abilitato Virtual Deliverability Manager per il tuo account, puoi definire impostazioni personalizzate per le modalità con cui un set di configurazione utilizzerà il monitoraggio del coinvolgimento e la consegna condivisa ottimizzata sovrascrivendo quelle definite in Virtual Deliverability Manager. Avrai così la flessibilità necessaria per personalizzare l'invio di e-mail per campagne specifiche. Ad esempio, puoi abilitare il monitoraggio del coinvolgimento e la consegna condivisa ottimizzata per le e-mail di marketing e disattivarli per le e-mail transazionali. Consulta le opzioni di Virtual Deliverability Manager durante la creazione o la modifica di un set di configurazione.

Iniziare a utilizzare Virtual Deliverability Manager tramite AWS CLI

Gli esempi seguenti illustrano le nozioni di base relative a Virtual Deliverability Manager tramite AWS CLI.

Per iniziare a usare Virtual Deliverability Manager tramite AWS CLI

Per iniziare a usare Virtual Deliverability Manager, esegui l'operazione `PutAccountVdmAttributes` nell'API Amazon SES v2. Puoi richiamare questa operazione da AWS CLI, come mostrato negli esempi seguenti.

- Abilita Virtual Deliverability Manager nel tuo account:

```
aws --region us-east-1 sesv2 put-account-vdm-attributes --vdm-attributes
 VdmEnabled=ENABLED
```

- Abilita il monitoraggio del coinvolgimento e la consegna condivisa ottimizzata tramite un file di input:

```
aws --region us-east-1 sesv2 put-account-vdm-attributes --cli-input-json file://
attributes.json
```

Il file di input sarà simile al seguente:

```
{
    "VdmAttributes": {
        "VdmEnabled": "ENABLED",
        "DashboardAttributes": {
            "EngagementMetrics": "ENABLED"
        },
        "GuardianAttributes": {
            "OptimizedSharedDelivery": "ENABLED"
        }
    }
}
```

Puoi trovare i valori dei parametri e i tipi di dati correlati collegandoti dal tipo di dati `VdmAttributes` nel riferimento nell'API Amazon SES v2.

> **Note**
>
> Attivando il monitoraggio del coinvolgimento, i tuoi URL e link vengono modificati in modo da includere i wrapper di tracciamento del coinvolgimento di Amazon SES.

> **Important**
>
> La consegna condivisa ottimizzata potrebbe comportare ritardi nell'invio delle e-mail, volti a proteggere la tua reputazione di invio. Se hai un carico di lavoro critico che deve essere inviato senza ritardi, ti consigliamo di non abilitare questa impostazione. Utilizza invece i set di configurazione per l'invio e abilita la consegna condivisa ottimizzata solo per quei set di configurazione per cui sono ammissibili ritardi.

- Per verificare il risultato:

```
aws --region us-east-1 sesv2 get-account
```

- Per definire impostazioni personalizzate per le modalità con cui un set di configurazione utilizzerà il monitoraggio del coinvolgimento e la consegna condivisa ottimizzata sovrascrivendo quelle definite in Virtual Deliverability Manager, consulta l'esempio AWS CLI in the section called “Impostazioni”.

Dashboard di Virtual Deliverability Manager

Il pannello di controllo offre una visione generale del programma dell'efficacia del recapito del tuo account, ad esempio con schede e grafici delle serie temporali di facile lettura che mostrano l'efficacia del recapito e la reputazione attraverso le velocità di apertura/clic e distribuzione e le statistiche di mancati recapiti/reclami. La dashboard offre anche una visione più dettagliata, utile per accedere a tabelle con dati specifici e più particolareggiati in caso di problemi legati a particolari ISP, identità di invio o set di configurazione associati a una campagna e-mail.

Grazie alla possibilità di avere una visione generale e poter anche approfondire con dettagli specifici, puoi concentrarti sulle aree problematiche per l'efficacia del recapito, anziché dover rivedere il programma di posta elettronica nel suo insieme. Questo livello di conoscenza consente inoltre di cogliere tendenze e possibili difficoltà prima che si trasformino in problemi di recapito più seri, come rinvii o blocchi.

Una panoramica dell'account nel pannello di controllo di Gestore virtuale della deliverability delle email che mostra le schede e i grafici delle serie temporali.

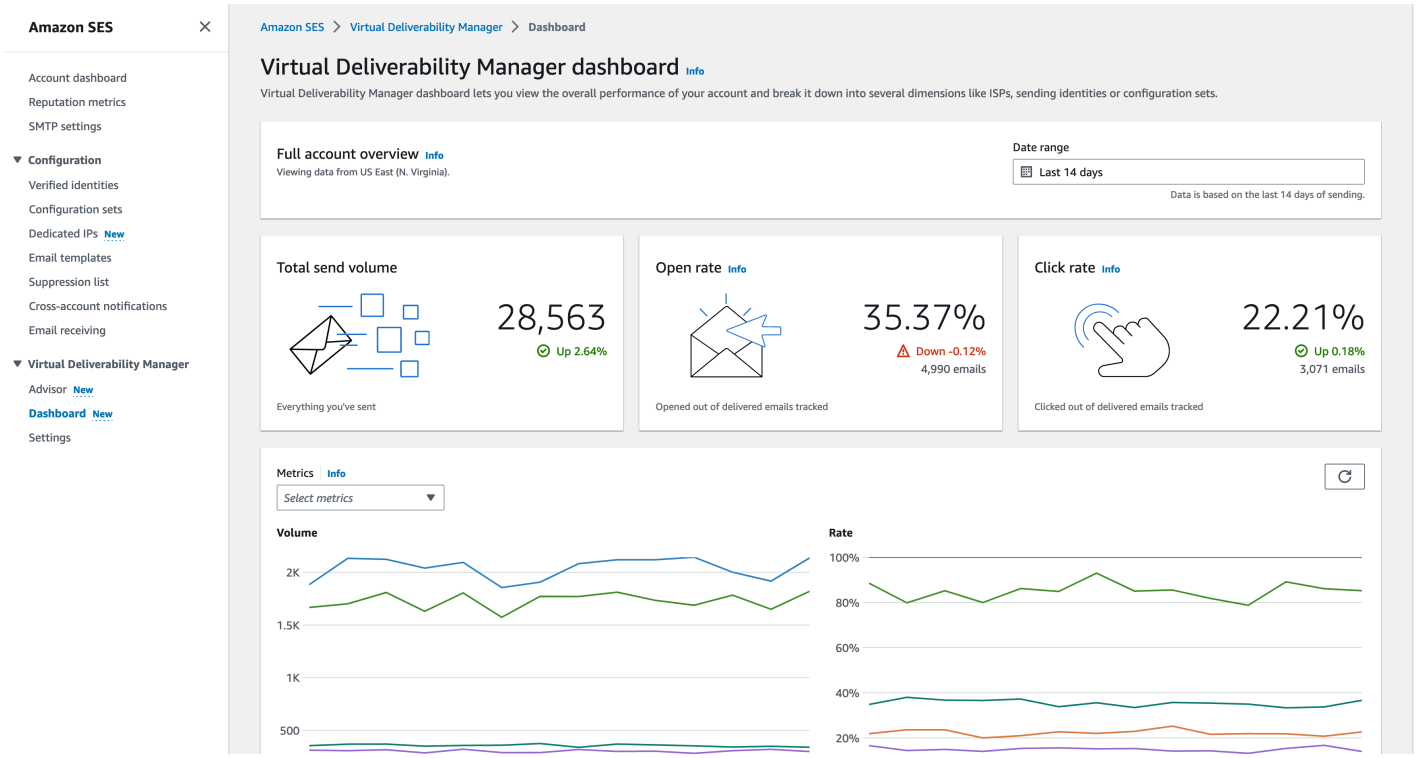
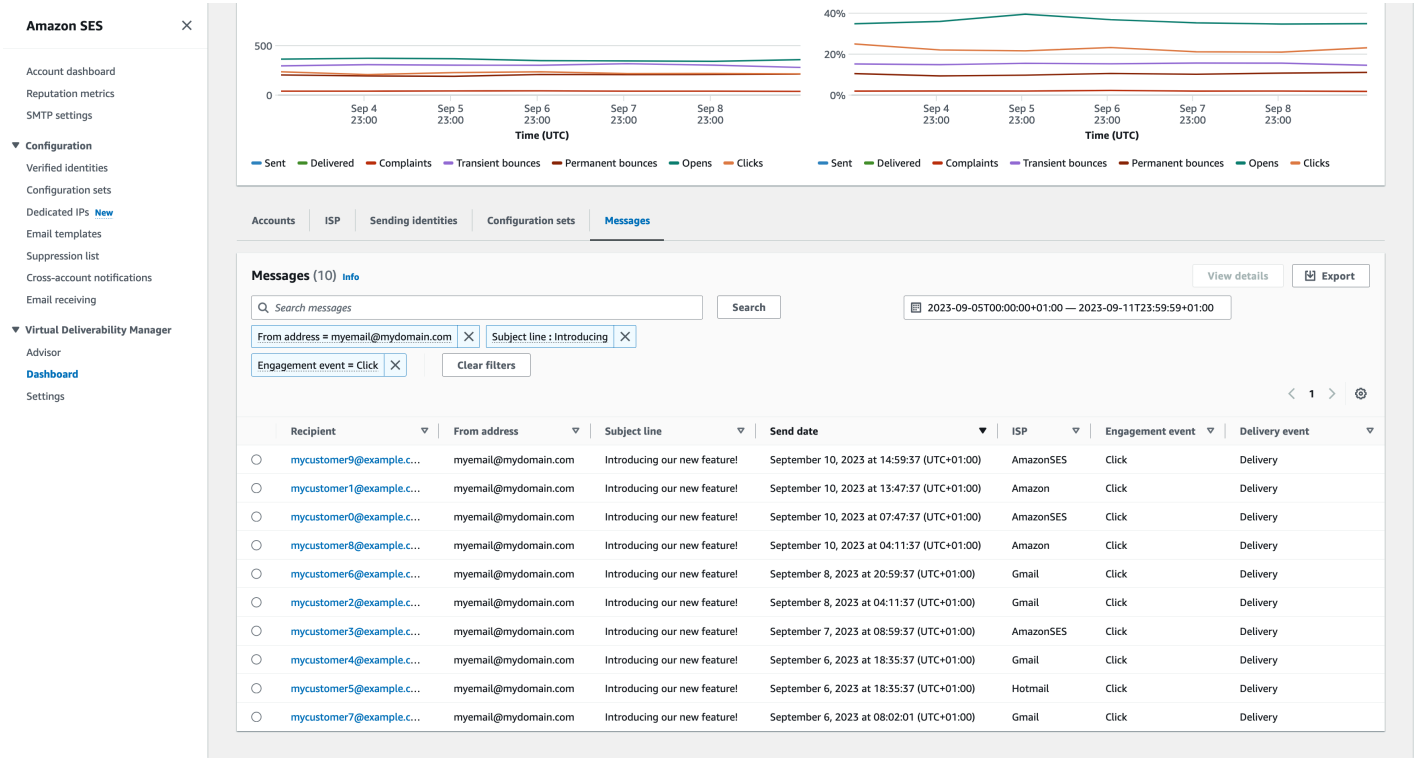


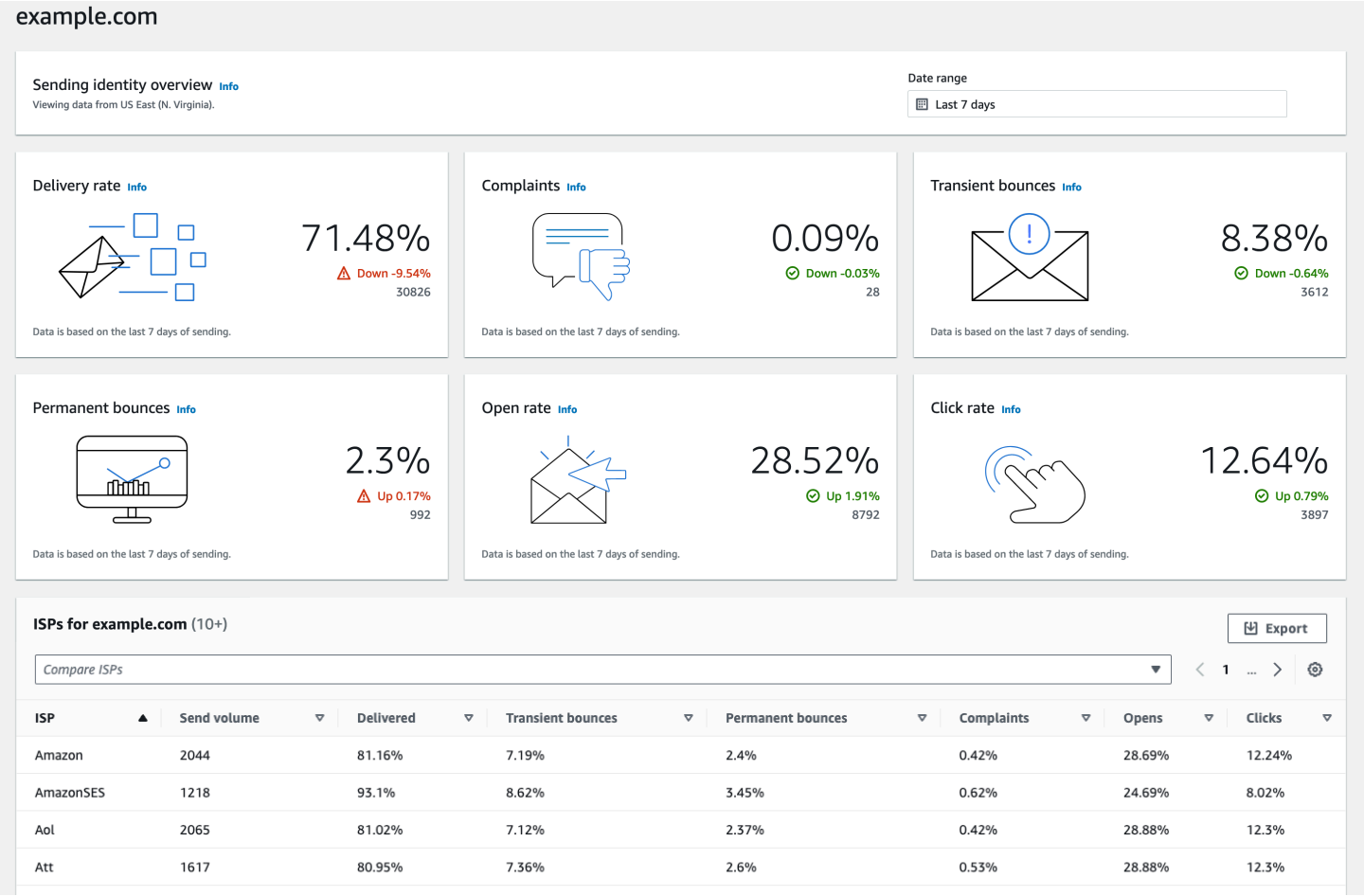
Tabella Messaggi selezionata nella dashboard di Gestore virtuale della deliverability delle email che mostra i messaggi inviati che corrispondono all'intervallo di date e ai criteri di filtro.



I dati particolareggiati forniti dalla dashboard possono essere utili per migliorare la tua reputazione come mittente e per calcolare orari e date ideali per ottimizzare il coinvolgimento e le conversioni del programma di posta elettronica con la possibilità di approfondire set di dati specifici:

- Dati ISP: utili in caso di problemi di recapito a uno specifico ISP o provider di mailbox. Invece di cercare di modificare l'intero account, che non avrebbe altri problemi, è possibile concentrarsi sull'endpoint problematico e allinearsi alle sue best practice per migliorare la reputazione del mittente per quell'ISP e ripristinare una buona efficacia del recapito nella posta in arrivo per raggiungere i tuoi destinatari. È anche importante comprendere la distribuzione dei tuoi ISP, perché potresti effettuare più invii a un ISP o a un provider di mailbox che ad altri. Per ottenere un impatto positivo sulla conversione delle tue e-mail, devi assicurarti che il traffico venga sempre recapitato e che i destinatari finali interagiscano con esso.
- Identità di invio e set di configurazione: utile per aiutarti a individuare le identità di invio e i set di configurazione che contribuiscono al problema di efficacia del recapito in generale per l'account. Puoi concentrarti su questi aspetti nello specifico, modificare le configurazioni ed eventualmente ridurre l'invio con una determinata identità fino alla risoluzione del problema. Prendiamo ad esempio un'identità di invio inserita per errore in un elenco di soppressione, con il risultato di far passare tutto il traffico attraverso quell'identità. Tale identità è associata a un set di configurazione e causa problemi di efficacia del recapito. In questi casi è utile poter individuare l'identità di invio o il set di configurazione in modo da potersi concentrare sulla risoluzione specifica del problema, anziché esaminare l'intero account per cercare di identificare la causa principale del problema di recapito.

Dati dettagliati mostrati nel pannello di controllo di Gestore virtuale della deliverability delle email per l'identità di invio selezionata, le schede example.com mostrano le metriche relative a efficacia del recapito e reputazione. La tabella mostra tutti gli ISP a cui l'identità di invio ha inviato posta con le percentuali dei parametri per ogni ISP all'interno dell'intervallo di date inserito.



Utilizzo della dashboard di Virtual Deliverability Manager nella console Amazon SES

La procedura seguente mostra come utilizzare la dashboard di Virtual Deliverability Manager nella console di Amazon SES per visualizzare le statistiche complessive di efficacia del recapito e reputazione e per approfondire le aree problematiche.

Per visualizzare i dati generali e più dettagliati relativi ai parametri di efficacia del recapito per il tuo account grazie alla dashboard di Virtual Deliverability Manager

1. Accedi AWS Management Console e apri la console Amazon SES all'indirizzo https://console.aws.amazon.com/ses/.
2. Nel riquadro di navigazione a sinistra, scegli Dashboard in Virtual Deliverability Manager.

> **Note**
>
> Se non hai abilitato Virtual Deliverability Manager per il tuo account, la Dashboard non sarà visibile. Per ulteriori informazioni, consulta the section called “Nozioni di base”.

3. Nel pannello Panoramica completa dell'account, scegli un intervallo di date da utilizzare per tutti le metriche nelle schede, nelle serie temporali e nelle tabelle di approfondimento.

   - Nel campo Date range (Intervallo di date), scegli Relative range (Intervallo relativo) (impostazione predefinita) o Absolute range (Intervallo assoluto).

     - Relative range (Intervallo relativo): seleziona il pulsante di opzione che corrisponde al numero di giorni desiderato.
       - Intervallo personalizzato: inserisci un intervallo in giorni (fino a 60), settimane (fino a 8) o mesi (fino a 2).
     - Intervallo assoluto: la prima data scelta sarà la data di inizio, la seconda data sarà la data di fine, per un massimo di 60 giorni totali. Per specificare un singolo giorno, sceglilo sia come data di inizio che di fine.

   > **Note**
   >
   > Quanto segue si applica a tutti gli intervalli di date nella dashboard:
   >
   > - Date e orari sono tutti UTC.
   > - Per le date in Relative range (Intervallo relativo), l'ultimo giorno termina con la mezzanotte UTC. Ad esempio, se scegli Last 7 days (Ultimi 7 giorni), il settimo giorno sarà ieri, con termine a mezzanotte.
   > - Se l'intervallo di date è superiore a 30 giorni, la colonna Differenza % nella tabella Statistiche dell'account e le percentuali di modifica nelle schede non avranno un valore (indicato da un trattino -).

4. Le schede, le serie temporali e tutte le tabelle di approfondimento, ovvero Statistiche account, ISP, Identità di invio e Set di configurazione, visualizzano i totali delle metriche calcolate in base all'intervallo di date inserito e utilizzano la matematica delle metriche descritta in Metodo di calcolo per i parametri della dashboard.

- Per creare un file `.csv` locale dei dati che stai visualizzando nella tabella ISP, Identità di invio o Set di configurazione, seleziona il relativo pulsante Esporta.

5. I grafici delle serie temporali che illustrano l'avanzamento di Volume e Percentuale per l'intervallo di date inserito vengono visualizzati nel pannello Parametri. Quando si passa il mouse su un intervallo di date nei grafici, verrà visualizzato il conteggio del volume o la percentuale della frequenza esatti in base a un'aggregazione giornaliera. Puoi filtrare i parametri che desideri visualizzare utilizzando il menu a discesa Seleziona parametri.
6. Scegli la scheda Accounts (Account) per visualizzare la tabella Accounts statistics (Statistiche account).

   - Questa tabella offre una panoramica dei parametri relativi a efficacia del recapito e reputazione, mostrando i valori totali di Volume, % Rate (Tasso in %) e % Difference (Differenza in %) per Sent (Inviati), Delivered (Recapitati), Complaints (Reclami), Transient & Permanent bounces (Mancati recapiti temporanei e permanenti), Opens & Clicks (Aperture e clic), in base ai calcoli per l'intervallo di date specificato.

   > **Note**
   >
   > Se l'intervallo di date è superiore a 30 giorni, la colonna Differenza % non avrà un valore (indicato da un trattino `-`).

7. Scegli la scheda ISP per visualizzare la tabella ISP.

   - Questa tabella mostra i parametri per Send volume (Volume invio), Delivered (Recapitati), Transient & Permanent bounces (Mancati recapiti temporanei e permanenti), Complaints (Reclami), Opens & Clicks (Aperture e clic) per ogni ISP a cui hai effettuato invii, in base ai calcoli per l'intervallo di date specificato.
   - Per applicare filtri in base a determinati ISP, nella casella di ricerca Confronta ISP, scegli la casella di controllo corrispondente a ogni ISP da includere.
   - Per creare un file `.csv` locale dei dati che stai attualmente visualizzando in questa tabella, seleziona il relativo pulsante Esporta.

8. Scegli la scheda Sending identities (Identità di invio) per visualizzare la tabella Sending identities (Identità di invio).

   - Questa tabella mostra i parametri per Send volume (Volume invio), Delivered (Recapitati), Transient & Permanent bounces (Mancati recapiti temporanei e permanenti), Complaints

(Reclami), Opens & Clicks (Aperture e clic) per ogni identità di invio utilizzata, in base ai calcoli per l'intervallo di date specificato.

- Per applicare filtri in base a determinate identità di invio, nella casella di ricerca Confronta le identità, scegli la casella di controllo corrispondente a ogni identità da includere.
- Per visualizzare in dettaglio un'identità di invio specifica, scegline il nome nella colonna Sending identity (Identità di invio).
  - Si apriranno le schede con informazioni su Velocità di consegna, Reclami, Mancati recapiti temporanei e permanenti, Tassi di apertura e clic per l'identità di invio selezionata, in base ai calcoli per l'intervallo di date specificato.
  - I grafici delle serie temporali verranno aggiornati mostrando tutti i parametri per l'identità di invio selezionata calcolata in base all'intervallo di date inserito.
  - Verrà visualizzata una tabella con tutti gli ISP a cui l'identità di invio ha inviato messaggi, con indicati i parametri per ciascun ISP, in base ai calcoli per l'intervallo di date specificato.
- Per creare un file `.csv` locale dei dati che stai attualmente visualizzando in questa tabella, seleziona il relativo pulsante Esporta.

9. Scegli la scheda Configuration sets (Set di configurazione) per visualizzare la tabella Configuration sets (Set di configurazione).

   - Questa tabella mostra i parametri per Send volume (Volume invio), Delivered (Recapitati), Transient & Permanent bounces (Mancati recapiti temporanei e permanenti), Complaints (Reclami), Opens & Clicks (Aperture e clic) per ogni set di configurazione utilizzato per inviare posta, in base ai calcoli per l'intervallo di date specificato.
   - Per applicare filtri in base a specifici set di configurazione, nella casella di ricerca Confronta i set di configurazione, scegli la casella di controllo corrispondente per ogni set di configurazione da includere.
   - Per approfondire un set di configurazione specifico, scegline il nome nella colonna Configuration set (Set di configurazione).
     - Si apriranno le schede con informazioni su Velocità di consegna, Reclami, Mancati recapiti temporanei e permanenti, Tassi di apertura e clic per il set di configurazione selezionato, in base ai calcoli per l'intervallo di date specificato.
     - I grafici delle serie temporali verranno aggiornati mostrando tutti i parametri per la configurazione selezionata calcolata in base all'intervallo di date inserito.

    - Verrà visualizzata una tabella con tutti gli ISP ai quali sono stati inviati messaggi utilizzando il set di configurazione, con indicati i parametri per ciascun ISP, in base ai calcoli per l'intervallo di date specificato.
- Per creare un file `.csv` locale dei dati che stai attualmente visualizzando in questa tabella, seleziona il relativo pulsante Esporta.

10. Scegli la scheda Messaggi per visualizzare la tabella Messaggi.

    Si tratta di una tabella interattiva che fornisce un modo per cercare e trovare i messaggi inviati. Per ciascun messaggio, puoi tenere traccia dello stato attuale di recapito e interazione, della cronologia degli eventi e visualizzare la risposta restituita dal fornitore di casella di posta. I seguenti punti illustrano i modi in cui è possibile cercare messaggi particolari:

    - Selezionando all'interno del selettore dell'intervallo di date, puoi filtrare i messaggi che hai inviato negli ultimi 30 giorni. Se non selezioni un intervallo di date, per impostazione predefinita la ricerca verrà eseguita sugli ultimi 7 giorni, incluso il giorno corrente all'interno del fuso orario.
    - Nel campo Messaggi di ricerca puoi filtrare in base a Destinatario, Indirizzo mittente, Oggetto, ISP, Evento di coinvolgimento, Evento di consegna, e ID messaggio; si applicano le seguenti proprietà:
        - A seconda del tipo di filtro, immettere una stringa di testo con distinzione tra maiuscole e minuscole o selezionare un valore da un elenco.
        - Evento di coinvolgimento è limitato a un singolo valore, Oggetto può avere fino a due valori e tutti gli altri filtri possono avere fino a cinque valori per ricerca. Filtrando per ID messaggio si escluderanno tutti gli altri filtri che possono essere stati selezionati, incluso l'intervallo di date.
        - La colonna ID messaggio è nascosta per impostazione predefinita, ma può essere visualizzata selezionando l'icona a forma di ingranaggio per personalizzare la modalità di visualizzazione della tabella Messaggi.
    - Dopo aver selezionato i filtri e l'intervallo di date, scegli Cerca; la tabella verrà popolata con i messaggi corrispondenti ai criteri di ricerca. La tabella può caricare fino a 100 messaggi. Se la ricerca restituisce più di 100 messaggi, i 100 messaggi nella tabella rappresentano un esempio casuale del totale restituito.
    - La selezione del pulsante di opzione di un messaggio e dell'opzione Visualizza dettagli visualizzerà una barra laterale Informazioni sul messaggio contenente i dettagli della cronologia completa degli eventi del messaggio, l'evento più recente in alto, e tutte le risposte o i codici diagnostici restituiti dal provider della casella postale.

- Per creare un file `.csv` locale dei dati che stai attualmente visualizzando in questa tabella, seleziona il relativo pulsante Esporta.

Accesso ai dati dei parametri di Virtual Deliverability Manager tramite AWS CLI

Gli esempi seguenti illustrano come accedere ai ai dati dei parametri di Virtual Deliverability Manager tramite AWS CLI. Si tratta degli stessi dati utilizzati nella dashboard di Virtual Deliverability Manager nella console.

Per accedere ai dati delle metriche di deliverability utilizzando il AWS CLI

Puoi utilizzare l'operazione `BatchGetMetricData` nell'API Amazon SES v2 per accedere ai dati dei parametri sull'efficacia del recapito. Puoi richiamare questa operazione da AWS CLI , come mostrato negli esempi seguenti.

- Per accedere ai dati dei parametri sull'efficacia del recapito:

```
aws --region us-east-1 sesv2 batch-get-metric-data --cli-input-json file://sends.json
```

- Il file di input sarà simile al seguente:

```
{
 "Queries": [
   {
     "Id": "Retrieve-Account-Sends",
     "Namespace": "VDM",
     "Metric": "SEND",
     "StartDate": "2022-11-04T00:00:00",
     "EndDate": "2022-11-05T00:00:00"
    }
 ]
}
```

Maggiori informazioni sui valori dei parametri e i tipi di dati correlati sono reperibili collegandosi dal tipo di dati `BatchGetMetricDataQuery` nel riferimento nell'API Amazon SES v2.

Filtrare ed esportare i dati delle metriche di deliverability utilizzando il AWS CLI

Questo esempio mostra come utilizzare l'operazione `CreateExportJob` per filtrare ed esportare i dati dei parametri di deliverability in un file .csv o .json utilizzando la AWS CLI. Si tratta degli stessi dati utilizzati nelle tabelle ISP, Identità di invio e Set di configurazione della dashboard del Gestore virtuale della deliverability delle email.

Per filtrare ed esportare i dati delle metriche di deliverability in un file.csv o .json utilizzando il AWS CLI

Puoi utilizzare l'operazione `CreateExportJob` insieme al tipo di dati `MetricsDataSource` nell'API v2 di Amazon SES per filtrare ed esportare i dati dei parametri in un file .csv o .json. Questa operazione viene richiamata da come illustrato nell'esempio seguente AWS CLI .

- Filtrare ed esportare i dati dei parametri di deliverability utilizzando un file di input:

```
aws --region us-east-1 sesv2 create-export-job --cli-input-json file://metric-export-input.json
```

- In questo esempio, il file di input utilizza i parametri `MetricsDataSource` da filtrare in base a tutti gli ISP a cui è stata inviata posta, che mostra la percentuale di consegna riuscita entro l'intervallo di date specificato e un formato .csv specificato per il file di output:

```
{
    "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"
    }
}
```

Maggiori informazioni sui valori dei parametri e i tipi di dati correlati sono disponibili in `MetricsDataSource` come un oggetto del tipo `ExportDataSource` nella documentazione di riferimento delle API v2 Amazon SES.

Individuazione dei messaggi inviati, del relativo stato di consegna e coinvolgimento ed esportazione dei risultati utilizzando il AWS CLI

In questi esempi viene mostrato come utilizzare l'operazione `CreateExportJob` per cercare e trovare determinati messaggi che hai inviato, visualizzare il relativo stato di consegna e coinvolgimento ed esportare i risultati della ricerca in un file .csv o .json utilizzando la AWS CLI. Si tratta degli stessi dati utilizzati nella tabella Messaggi della dashboard di Gestore virtuale della deliverability delle email.

Per trovare i messaggi inviati, il relativo stato di consegna e coinvolgimento ed esportare i risultati in un file.csv o .json utilizzando il AWS CLI

Puoi utilizzare l'operazione `CreateExportJob` insieme al tipo di dati `MessageInsightsDataSource` nell'API v2 Amazon SES per applicare filtri per trovare messaggi particolari che hai inviato, visualizzare il relativo stato di consegna e coinvolgimento ed esportare i risultati in un file.csv o .json. Questa operazione viene richiamata da AWS CLI come illustrato negli esempi seguenti.

> **Note**
>
> Se la ricerca filtrata restituisce più di 10.000 messaggi, i 10.000 messaggi nel set di risultati dell'API rappresentano un esempio casuale del totale restituito.

- Trova i messaggi inviati, visualizza il relativo stato attuale ed esporta i risultati utilizzando un file di input:

```
aws --region us-east-1 sesv2 create-export-job --cli-input-json file://message-insights-export-input.json
```

- In questo esempio, il file di input utilizza i parametri `MessageInsightsDataSource` per filtrare in base a un soggetto uguale a “I saldi terminano stasera!” e un formato .csv specificato per il file di output:

```
{
    "ExportDataSource": {
        "MessageInsightsDataSource": {
            "StartDate": "2023-07-01T00:00:00",
            "EndDate": "2023-07-10T00:00:00",
            "Include": {
                "Subject": [
                    "Sale Ends Tonight!"
                ]
            }
        }
    },
    "ExportDestination": {
        "DataFormat": "CSV"
    }
}
```

- In questo esempio, il file di input utilizza `MessageInsightsDataSource`parametri per filtrare in base a un argomento che inizia con «Hello», inviato con una «informazione» FromEmailAddress contenente una «informazione» a destinazioni che terminano con «@example .com» e un formato.json specificato per il file di output:

```
{
    "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"
    }
}
```

- In questo esempio, il file di input utilizza `MessageInsightsDataSource`parametri per filtrare un oggetto che inizia con «Hello», esclude i risultati con "noreply@example.com" come formato e un FromEmailAddress formato.csv specificato per il file di output:

```
{
    "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"
    }
}
```

- In questo esempio, il file di input utilizza `MessageInsightsDataSource`parametri per filtrare in base a un argomento che inizia con «Hello», inviato con una «informazione» FromEmailAddress contenente a destinazioni che terminano con «@example .com», utilizza Gmail come ISP, un ultimo evento di consegna di «DELIVERY», un ultimo evento di coinvolgimento che è «OPEN» o «CLICK» e un formato.json specificato per il file di output:

```
{
    "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"
    }
}
```

- In questo esempio, il file di input utilizza `MessageInsightsDataSource`parametri per filtrare le destinazioni che terminano con «@example1 .com», «@example2 .com» o «@example3 .com», esclude i messaggi con un LastDeliveryEvent valore uguale a «SEND» o «DELIVERY» e un formato.csv specificato per il file di output:

```
{
    "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"
    }
}
```

Maggiori informazioni sui valori dei parametri e i tipi di dati correlati sono disponibili in `MessageInsightsDataSource` come un oggetto del tipo `ExportDataSource` nella documentazione di riferimento delle API v2 Amazon SES.

Gestione dei processi di esportazione utilizzando la AWS CLI

In questi esempi viene illustrato come gestire i processi di esportazione elencandoli, ottenendo informazioni su di essi e annullandoli utilizzando la AWS CLI.

Per elencare i lavori di esportazione, utilizzare il AWS CLI

Puoi utilizzare l'operazione `ListExportJobs` nell'API v2 Amazon SES per elencare i processi di esportazione. È possibile richiamare questa operazione da AWS CLI come illustrato negli esempi seguenti.

- Elenca i tuoi processi di esportazione:

```
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
```

- Il file di input sarà simile al seguente:

```
{
  "NextToken": "",
  "PageSize": 0,
  "ExportSourceType": "METRICS_DATA",
  "JobStatus": "CREATED"
}
```

Ulteriori informazioni sui valori dei parametri per l'operazione `ListExportJobs` sono disponibili nella documentazione di riferimento delle API v2 Amazon SES.

Per ottenere informazioni sul processo di esportazione, utilizza il AWS CLI

Puoi utilizzare l'operazione `GetExportJob` nell'API v2 Amazon SES per ottenere informazioni sul processo di esportazione. È possibile richiamare questa operazione da AWS CLI come illustrato negli esempi seguenti.

- Ottieni informazioni sul processo di esportazione:

```
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
```

- Il file di input sarà simile al seguente:

```
{
    "JobId": "e2220d6b-dce5-45f2-bf60-3287a465b732"
}
```

Ulteriori informazioni sui valori dei parametri per l'operazione `GetExportJob` sono disponibili nella documentazione di riferimento delle API v2 Amazon SES.

Per annullare il processo di esportazione, utilizzare il AWS CLI

Puoi utilizzare l'operazione `CancelExportJob` nell'API v2 Amazon SES per annullare il processo di esportazione. È possibile richiamare questa operazione da AWS CLI come illustrato negli esempi seguenti.

- Annulla il processo di esportazione:

```
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
```

- Il file di input sarà simile al seguente:

```
{
    "JobId": "e2220d6b-dce5-45f2-bf60-3287a465b732"
}
```

  Ulteriori informazioni sui valori dei parametri per l'operazione `CancelExportJob` sono disponibili nella documentazione di riferimento delle API v2 Amazon SES.

Visualizzazione della cronologia completa degli eventi di un messaggio e delle risposte dell'ISP utilizzando il AWS CLI

Nell'esempio seguente viene mostrato come visualizzare i dettagli della cronologia eventi completa di un messaggio e tutte le risposte o i codici diagnostici restituiti dal provider della casella postale utilizzando la AWS CLI. Si tratta degli stessi dati utilizzati nella barra laterale Informazioni sul messaggio dopo aver selezionato il pulsante di opzione di un messaggio nella tabella Messaggi della dashboard del Gestore virtuale della deliverability delle email.

Per visualizzare la cronologia degli eventi di un messaggio e le risposte dell'ISP, utilizzare AWS CLI

Puoi utilizzare l'operazione `GetMessageInsights` nell'API v2 Amazon SES per visualizzare i dettagli di un messaggio inviato. È possibile richiamare questa operazione da AWS CLI come illustrato nell'esempio seguente.

- Visualizza i dettagli del messaggio su un'e-mail inviata identificata dal relativo message-id:

```
aws --region us-east-1 sesv2 get-message-insights --message-id
 01000100001000dd-2a19190d-99d4-0000-9f00-deb5bbf2bfbe-000001
```

Ulteriori informazioni sui valori dei parametri per l'operazione `GetMessageInsights` sono disponibili nella documentazione di riferimento delle API v2 Amazon SES.

Metodo di calcolo per i parametri della dashboard di Virtual Deliverability Manager

Tutte le schede dei tassi e le tabelle dettagliate mostrate nel pannello di controllo di Gestore virtuale della deliverability delle email calcolano le metriche per l'intervallo di date specificato nel pannello Panoramica completa dell'account.

Le percentuali dei tassi dei parametri mostrati nella dashboard vengono calcolati come descritto nella tabella. Le ultime quattro colonne rappresentano i qualificatori per la matematica di base utilizzata per derivare i parametri visualizzate. Ad esempio, il tasso di apertura viene calcolato come il totale delle aperture diviso per il totale recapitato relativo ai messaggi HTML recapitati con il monitoraggio del coinvolgimento attivato. Non includono i messaggi inviati senza il monitoraggio del coinvolgimento e senza codifica HTML.

Percentuale del tasso	Metodo di calcolo	Con tracciamento del coinvolgimento abilitato e HTML	E con almeno 1 link tracciato	Consegna o agli ISP con FBL SES	Escluso se inserito in elenco di eliminazioni a livello di account
Percentuale di aperture	totale aperto/totale recapitato	✗			
Percentuale di clic	totale clic/totale recapitato	✗	✗		

Percentuale del tasso	Metodo di calcolo	Con tracciamento del coinvolgimento abilitato e HTML	E con almeno 1 link tracciato	Consegnato agli ISP con FBL SES	Escluso se inserito in elenco di eliminazioni a livello di account
Complaint rate (Percentuale di reclami)	totale reclami/totale recapitato			✗	✗
Percentuale di recapiti	totale recapitato/totale inviato				
Percentuale mancati recapiti temporanei	totale mancati recapiti temporanei/totale inviato				✗
Percentuale mancati recapiti permanenti	totale mancati recapiti permanenti/totale inviato				✗
Volume di invio totale	Percentuale del tasso non visualizzata (tutto ciò che hai inviato; sempre 100%)				

Metodo di calcolo del tasso di differenza e dei totali del volume per tutti i parametri:

- % differenza: differenza nel totale del parametro rispetto al totale precedente del parametro per l'intervallo di date specificato. Ad esempio, se l'intervallo di date specificato è Last 7 days (Ultimi 7 giorni): tasso del parametro negli ultimi 7 giorni - tasso del parametro nei 7 giorni precedenti.

- La percentuale di differenza per il volume totale di invio viene calcolata in modo diverso. Ad esempio, (Volume di invio degli ultimi 7 giorni - Volume di invio dei 7 giorni precedenti)/Volume di invio dei 7 giorni precedenti.

- Volume: conteggio totale di ogni parametro.

> **Note**
>
> - La colonna Delivered (Recapitato) nelle tabelle di approfondimento mostra il semplice volume recapitato, senza i qualificatori di recapito utilizzati per il calcolo delle percentuali di apertura, clic e reclami.
> - Virtual Deliverability Manager tiene traccia dei parametri derivanti solo dalle e-mail con un unico destinatario: le e-mail con più destinatari non vengono conteggiate in nessun parametro della dashboard di Virtual Deliverability Manager.
>   - In questi casi, i conteggi dei parametri di Virtual Deliverability Manager saranno inferiori ai conteggi dei parametri di Amazon CloudWatch perché i CloudWatch parametri includono e-mail con più destinatari.
> - Le e-mail inviate al simulatore di mailbox di SES non vengono conteggiate in nessun parametro della dashboard di Virtual Deliverability Manager.
> - Le e-mail inviate tramite l'account di un mittente delegato (in precedenza invio tra account) non vengono conteggiate in nessuna delle metriche della dashboard del Gestore virtuale della deliverability delle email.

> **Important**
>
> Protezione della privacy di Mail su Apple ed effetto sulle percentuali di coinvolgimento: a seguito dell'implementazione della funzionalità Protezione della privacy di Mail (MPP) per i dispositivi Apple con iOS15 e superiori, i numeri relativi all'interazione risultano gonfiati, perché la funzionalità MPP attiva le aperture all'avvio dell'app Mail di Apple, non necessariamente quando un destinatario apre e/o fa clic su un messaggio. Il risultato è che i dati sul coinvolgimento risultano molto più alti di quanto sarebbero normalmente e questo è un aspetto di cui gli esperti di marketing e-mail devono tenere in considerazione quando esaminano il coinvolgimento. Esistono diversi altri modi per identificare il coinvolgimento, come l'attività web, l'utilizzo di app/portali e anche l'utilizzo di dati proxy provenienti da dispositivi non Apple per creare un parametro aggregato. La cosa importante su cui

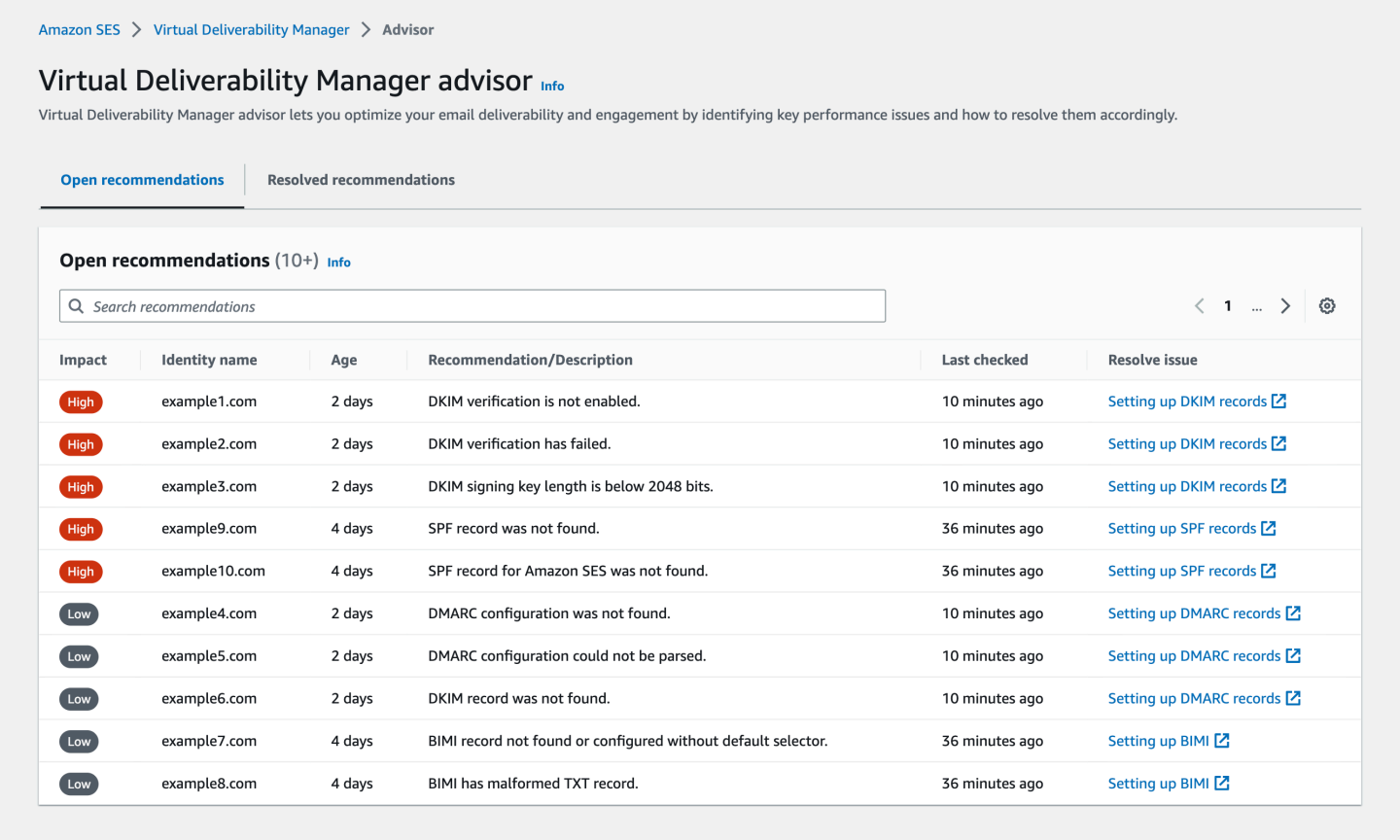
concentrarsi sono le tendenze del coinvolgimento, perché da esse possono emergere possibili problemi con l'invio di e-mail. Per ulteriori informazioni consulta la pagina Apple Mail's Privacy Protection (Protezione della privacy di Mail su Apple).

Advisor di Virtual Deliverability Manager

L'advisor di Virtual Deliverability Manager aiuta a ottimizzare il coinvolgimento e l'efficacia del recapito delle e-mail identificando i principali problemi di prestazioni e infrastruttura dell'account e inviando livelli di identità che influiscono negativamente sull'efficacia del recapito e sulla reputazione delle e-mail. Offre soluzioni tramite indicazioni specifiche su come risolvere il problema identificato.

I consigli dell'advisor sull'infrastruttura sono riportati nella tabella Open recommendations (Consigli aperti). Tali consigli identificano i problemi di autenticazione e-mail standard, ad esempio quando i record SPF, DKIM, DMARC o BIMI non esistono o presentano problemi di configurazione, come l'essere difettosi o avere una lunghezza della chiave troppo corta. e sono classificati in base alla gravità dell'impatto, al nome identità del dominio di invio e all'età dell'avviso. Nella barra di ricerca, una casella di elenco offre la possibilità di filtrare in base al livello di impatto, alla categoria dell'infrastruttura o al nome dell'identità di invio. La colonna Data ultimo controllo mostra l'ora relativa dell'ultimo aggiornamento del suggerimento, ad esempio "Proprio ora" o "15 minuti fa". Nell'ultima colonna, Resolve issue (Risolvi il problema), è riportato un link alla sezione pertinente della Guida per gli sviluppatori di Amazon SES con indicazioni su come risolvere il problema identificato.

I consigli aperti vengono visualizzati nell'advisor di Virtual Deliverability Manager, ordinati per livello di impatto.



In assenza di notifiche attive da parte dell'advisor, un messaggio indicherà che non hai consigli aperti. Ti consigliamo di consultare regolarmente l'advisor. Facoltativamente, puoi integrare questi eventi di notifica degli advisor con Amazon EventBridge per creare applicazioni scalabili basate sugli eventi, come spiegato in. Monitoraggio tramite EventBridge

Dalla pagina dell'advisor di Virtual Deliverability Manager puoi anche accedere alla tabella Resolved recommendations (Consigli risolti), che elenca i problemi dell'infrastruttura risolti implementando le linee guida offerte dall'advisor. I consigli risolti sono indicati con uno stato iniziale che descrive il problema prima della sua risoluzione. I consigli risolti scadono dopo 30 giorni.

Cosa cerca il consulente di Virtual Deliverability Manager

Nella sezione precedente abbiamo discusso del fatto che il consulente di Virtual Deliverability Manager esegue controlli sul dominio di invio per determinare se è stata configurata un'infrastruttura autenticata in modo sicuro per garantire un elevato tasso di recapito delle e-mail e mantenere una buona reputazione di mittente. Prima di attivare il consulente Virtual Deliverability Manager, riteniamo che sarebbe utile sapere esattamente cosa sta controllando il consulente e cosa cerca in tali controlli.

È possibile utilizzare questa tabella come riferimento per esaminare la configurazione del dominio di invio e correggere tutti questi elementi che non sono allineati agli standard elencati in questa tabella prima che diventino problemi di cui l'advisor deve avvisare l'utente.

Tipo di controllo	Messaggio del consulente	Perché il consulente ti sta avvisando	Ulteriori informazioni
Configurazione DKIM	La verifica DKIM non è abilitata.	DKIM non è abilitato per identità.	DKIM semplificato in SES
La forza della chiave DKIM	La lunghezza della chiave di firma DKIM è inferiore a 2048 bit.	La lunghezza della chiave di firma DKIM non utilizza almeno 2048 bit.	DKIM semplificato in SES
Convalida dei record DNS DKIM	La verifica DKIM non è riuscita.	Record CNAME DKIM determinati non validi dopo aver cercato e provato a convalidare la chiave.	Verifica dell'identità di un dominio DKIM con il tuo provider DNS
Configurazione DMARC	La configurazione DMARC non è stata trovata.	Mancano i record DMARC TXT.	Configurazione della politica DMARC sul tuo dominio
Controllo del formato di registrazione DNS DMARC	La configurazione DMARC non può essere analizzata.	Formato non valido trovato per i record TXT DMARC.	Configurazione della politica DMARC sul tuo dominio
La configurazione DKIM di DMARC	Il record DKIM non è stato trovato.	Non è stato trovato alcun record DKIM conforme a DMARC.	Conformità a DMARC tramite DKIM
La configurazione DKIM di DMARC	Il record DKIM non è allineato.	Il dominio specificato nella firma DKIM non è allineato (corrispo nde) al dominio nell'indirizzo From.	Conformità a DMARC tramite DKIM

Tipo di controllo	Messaggio del consulente	Perché il consulente ti sta avvisando	Ulteriori informazioni
Configurazione SPF	Il record SPF non è stato trovato.	Record TXT SPF mancante per il dominio Custom MAIL FROM.	Configurazione del dominio MAIL FROM personalizzato
SPF «include» configurato	Il record SPF per Amazon SES non è stato trovato.	`include:amazonses.com` non è presente nel record TXT SPF.	Configurazione del dominio MAIL FROM personalizzato
Applicazione SPF configurata	Manca il qualificatore SPF all.	`~all`non è presente nel record TXT SPF.	Configurazione del dominio MAIL FROM personalizzato
Convalida dell'applicazione SPF	È stato rilevato un problema di configurazione SPF.	I tentativi di rilevare il record SPF MX richiesto entro 72 ore non sono riusciti.	Stati di configurazione del dominio MAIL FROM personalizzati
BIMI configurato	Record BIMI non trovato o configurato senza selettore predefinito.	I record BIMI TXT sono mancanti o mancano dell'attributo selector.	Configurazione di BIMI
Convalida del formato BIMI	BIMI ha un record TXT non valido.	Il record BIMI TXT è risultato configurato in modo errato dopo aver verificato la presenza e il formato valido di: versione, URL del certificato e URL del logo.	Configurazione di BIMI

Utilizzo dell'advisor di Virtual Deliverability Manager nella console Amazon SES

La procedura seguente illustra come utilizzare l'advisor di Virtual Deliverability Manager nella console Amazon SES per risolvere i problemi di consegna identificati tramite la console Amazon SES.

Per risolvere i problemi di efficacia del recapito e di reputazione tramite l'advisor di Virtual Deliverability Manager

1. Accedi AWS Management Console e apri la console Amazon SES all'indirizzo https://console.aws.amazon.com/ses/.
2. Nel riquadro di navigazione a sinistra, scegli Advisor in Virtual Deliverability Manager.

   > **Note**
   >
   > Se non hai abilitato Virtual Deliverability Manager per il tuo account, l'Advisor non sarà visibile. Per ulteriori informazioni, consulta the section called “Nozioni di base”.

3. Per impostazione predefinita, viene visualizzata la tabella Open recommendations (Consigli aperti). I consigli sono divisi in categorie per Impact (Impatto) (alto o basso), Identity name (Nome identità) (dominio di invio), Age (Età) (dell'avviso) e Recommendation/Description (Consiglio/descrizione) (problema identificato). Nella barra di ricerca, è possibile filtrare in base al livello di impatto (Impact), alla categoria (Category) del problema dell'infrastruttura o al nome dell'identità (Identity name) del dominio di invio.
4. Per risolvere un problema descritto nella colonna Recommendation/Description (Consiglio/Descrizione), scegli il link nella colonna Resolve issue (Risolvi problema) per quella riga e implementa la soluzione suggerita.

   > **Note**
   >
   > Dopo aver implementato una soluzione, sono necessarie fino a sei ore perché il problema risolto risulti come tale. Puoi visualizzare il problema risolto nella scheda Resolved recommendations (Consigli risolti).

Accesso ai consigli di Virtual Deliverability Manager tramite AWS CLI

Gli esempi seguenti illustrano come accedere ai consigli di Virtual Deliverability Manager tramite AWS CLI.

Per accedere ai consigli di Virtual Deliverability Manager utilizzando il AWS CLI

Puoi utilizzare l'operazione `ListRecommendations` nell'API Amazon SES v2 per un elenco dei consigli per l'efficacia del recapito. Puoi richiamare questa operazione da AWS CLI, come mostrato negli esempi seguenti.

- Per ottenere un elenco dei consigli e individuare i problemi di efficacia del recapito:

```
aws --region us-east-1 sesv2 list-recommendations
```

- Per applicare filtri e recuperare i consigli per un dominio specifico di tua proprietà:

```
aws --region us-east-1 sesv2 list-recommendations --cli-input-json file://list-
recommendations.json
```

- Il file di input sarà simile al seguente:

```
{
  "PageSize":100,
  "Filter":{
    "RESOURCE_ARN": "arn:aws:ses:us-east-1:123456789012:identity/example.com"
   }
}
```

Impostazioni di Virtual Deliverability Manager

Puoi visualizzare o modificare le impostazioni di Virtual Deliverability Manager nel tuo account in qualsiasi momento. Puoi abilitare o disabilitare Virtual Deliverability Manager, nonché specificare una modalità di attivazione o disattivazione per il monitoraggio del coinvolgimento e il recapito condiviso ottimizzato a livello di account Virtual Deliverability Manager tramite la console Amazon SES o AWS CLI

Le opzioni di Virtual Deliverability Manager sono disponibili anche a livello di set di configurazione; in questo modo, puoi definire impostazioni personalizzate per le modalità con cui un set di

configurazione utilizzerà il monitoraggio del coinvolgimento e il recapito condiviso ottimizzato sovrascrivendo quelle definite in Virtual Deliverability Manager. Avrai così la flessibilità necessaria per personalizzare l'invio di e-mail per campagne specifiche. Ad esempio puoi abilitare il monitoraggio del coinvolgimento e il recapito condiviso ottimizzato per le e-mail di marketing e disattivarli per le e-mail transazionali.

Modifica delle impostazioni dell'account Virtual Deliverability Manager tramite la console Amazon SES

La procedura seguente illustra come modificare le impostazioni dell'account Virtual Deliverability Manager tramite la console Amazon SES.

Per modificare le impostazioni dell'account Virtual Deliverability Manager tramite la console Amazon SES

1. Accedi alla AWS Management Console e apri la console Amazon SES all'indirizzo https://console.aws.amazon.com/ses/.
2. Nel riquadro di navigazione a sinistra, scegli Settings (Impostazioni) in Virtual Deliverability Manager.

   Si apre la pagina Virtual Deliverability Manager settings (Impostazioni di Virtual Deliverability Manager). Il pannello Subscription overview (Panoramica delle sottoscrizioni) indica lo stato di Virtual Deliverability Manager, mentre il pannello Additional settings (Impostazioni aggiuntive) mostra lo stato delle funzionalità Engagement tracking (Monitoraggio del coinvolgimento) e Optimized shared delivery (Recapito condiviso ottimizzato).
3. Per modificare le impostazioni Monitoraggio del coinvolgimento o Distribuzione condivisa ottimizzata:

   a. Nel pannello Additional settings (Impostazioni aggiuntive), scegli Edit (Modifica).

   b. Seleziona il pulsante di opzione corrispondente per attivare o disattivare una delle funzionalità, quindi scegli Submit settings (Invia impostazioni).

      La pagina Virtual Deliverability Manager settings (Impostazioni di Virtual Deliverability Manager) mostra un riepilogo delle modifiche nel pannello Additional settings (Impostazioni aggiuntive).

> **Note**
>
> Le opzioni Monitoraggio del coinvolgimento definite qui o nel set di configurazione di Virtual Deliverability Manager, controllano se segnalare aperture e clic nella dashboard di Virtual Deliverability Manager; non influiscono sulle configurazioni di destinazione degli eventi che pubblicano eventi di apertura e clic. Ad esempio, se il monitoraggio del coinvolgimento è stato disattivato, la pubblicazione dell'evento di apertura e clic impostato qui non verrà disattivato nelle destinazioni degli eventi SES.

4. (Facoltativo) Per definire impostazioni personalizzate per le modalità con cui un set di configurazione utilizza il monitoraggio del coinvolgimento e il recapito condiviso ottimizzato sovrascrivendo quelle definite in Virtual Deliverability Manager, consulta le opzioni di Virtual Deliverability Manager durante la creazione o la modifica di un set di configurazioni.
5. Per disabilitare Virtual Deliverability Manager:
   a. Nel pannello Subscription overview (Panoramica delle sottoscrizioni), scegli Disable Virtual Deliverability Manager (Disabilita Virtual Deliverability Manager).
   b. Nella finestra popup Disable Virtual Deliverability Manager? (Disabilitare Virtual Deliverability Manager?), inserisci *`Disable`* nel campo di conferma, quindi scegli Disable Virtual Deliverability Manager (Disabilita Virtual Deliverability Manager).
   c. Compare un banner che conferma la disabilitazione di Virtual Deliverability Manager.
6. Per abilitarlo nuovamente, consulta the section called “Nozioni di base”.

Modifica delle impostazioni dell'account Virtual Deliverability Manager tramite AWS CLI

Puoi modificare le impostazioni dell'account Virtual Deliverability Manager tramite AWS CLI.

Per modificare le impostazioni dell'account Virtual Deliverability Manager tramite AWS CLI

Per modificare le impostazioni di Virtual Deliverability Manager, puoi utilizzare le operazioni `PutAccountVdmAttributes` e `PutConfigurationSetVdmOptions` nell'API Amazon SES v2. Puoi richiamare questa operazione da AWS CLI, come mostrato negli esempi seguenti.

- Abilita o disabilita il monitoraggio del coinvolgimento, il recapito condiviso ottimizzato o entrambi tramite un file di input:

```
aws --region us-east-1 sesv2 put-account-vdm-attributes --cli-input-json file://
attributes.json
```

In questo esempio, in cui il monitoraggio del coinvolgimento è `ENABLED` e il recapito condiviso ottimizzato è `DISABLED`, il file di input si presenta in modo simile al seguente:

```
{
    "VdmAttributes": {
        "VdmEnabled": "ENABLED",
        "DashboardAttributes": {
            "EngagementMetrics": "ENABLED"
        },
        "GuardianAttributes": {
            "OptimizedSharedDelivery": "DISABLED"
        }
    }
}
```

Puoi trovare maggiori informazioni sui valori dei parametri e i tipi di dati correlati collegandoti dal tipo di dati `VdmAttributes` nel riferimento nell'API Amazon SES v2.

- Definisci impostazioni personalizzate per le modalità con cui un set di configurazione utilizzerà il monitoraggio del coinvolgimento e il recapito condiviso ottimizzato sovrascrivendo quelle definite in Virtual Deliverability Manager:

```
aws --region us-east-1 sesv2 put-configuration-set-vdm-options --cli-input-json
 file://config-set.json
```

In questo esempio, in cui un set denominato example ha abilitati sia il monitoraggio del coinvolgimento sia il recapito condiviso ottimizzato, il file di input si presenta in modo simile al seguente:

```
{
    "ConfigurationSetName": "example",
    "VdmOptions": {
        "DashboardOptions": {
            "EngagementMetrics": "ENABLED"
```

```
        },
        "GuardianOptions": {
            "OptimizedSharedDelivery": "ENABLED"
        }
    }
}
```

Per maggiori informazioni sui valori dei parametri e i tipi di dati correlati, consulta il tipo di dati `VdmOptions` nel riferimento nell'API Amazon SES v2.

- Per verificare il risultato:

```
aws –region us-east-1 sesv2 get-configuration-set –configuration-set-name example
```

- Se non viene specificata l'opzione `DashboardOptions` o `GuardianOptions` a livello di set di configurazione, al traffico inviato tramite quel set di configurazione vengono applicate le impostazioni specificate a livello di account Virtual Deliverability Manager.

Gestore di posta per Amazon SES

Mail Manager è un set di funzionalità del gateway e-mail di Amazon SES progettato per aiutarti a rafforzare l'infrastruttura e-mail della tua organizzazione, semplificare la gestione del flusso di lavoro e-mail e semplificare il controllo della conformità delle e-mail. Si integra con l'infrastruttura esistente, può connettere diverse applicazioni aziendali e automatizza l'elaborazione delle e-mail in entrata. Mail Manager funge anche da prima linea di difesa per mantenere un sistema di posta elettronica sano, gestendo in modo efficiente il traffico e-mail e migliorando la conformità grazie alla sua capacità di archiviazione delle e-mail.

Oltre alle attuali funzionalità di Amazon SES, Mail Manager include le seguenti funzionalità che supportano il traffico in entrata:

- Endpoint Ingress: un componente chiave dell'infrastruttura che utilizza policy e regole di filtraggio configurabili per determinare quali e-mail devono essere ammesse all'interno dell'organizzazione e quali rifiutate.
- Criteri e set di regole sul traffico: consenti agli amministratori di posta elettronica di definire e applicare regole per la gestione del traffico e-mail in entrata con policy e regole altamente personalizzabili in grado di ordinare, classificare, assegnare priorità ed eseguire azioni sulle e-mail in base a un ricco set di condizioni ed eccezioni definite dall'utente. Questo filtraggio intelligente combinato con flussi di lavoro automatizzati aiuta a semplificare la gestione delle e-mail, a migliorare l'efficienza e a garantire la conformità con le politiche aziendali relative alla posta elettronica.
- Inoltro SMTP: reindirizza il traffico e-mail verso altri server SMTP in base a criteri definiti nelle regole collegando i sistemi di posta elettronica interni e semplifica la gestione delle e-mail con l'inoltro automatico. La possibilità di distribuire il traffico su più server e gateway consente all'organizzazione di gestire efficacemente il traffico e-mail ad alto volume, anche in ambienti ibridi.
- Archiviazione delle e-mail: salva e protegge le e-mail archiviando i dati in uno spazio di archiviazione persistente e sicuro a lungo termine e offre un modo per cercare e archiviare rapidamente le e-mail. Fornisce un'archiviazione a tempo pieno a livello aziendale senza aumentare i requisiti di archiviazione del server di casella di posta.
- Componenti aggiuntivi per la posta elettronica: una raccolta di strumenti di sicurezza specializzati, forniti da fornitori approvati da SES, che possono essere utilizzati per gestire le e-mail che arrivano all'endpoint di ingresso e per fornire opzioni di routing basate sui risultati di sicurezza. Questi strumenti sono soluzioni certificate di intelligence e applicazione della sicurezza pronte per essere

integrate nel flusso di lavoro di posta elettronica e possono essere attivate direttamente dalla console di Mail Manager.

Guida introduttiva a Mail Manager

Per iniziare a utilizzare Mail Manager, una procedura guidata di onboarding nella console Amazon SES ti guiderà attraverso i passaggi per abilitare Mail Manager per il tuo account. Per informazioni, consulta the section called “Nozioni di base”.

Argomenti

Guida introduttiva a Mail Manager

Per iniziare a utilizzare Amazon SES Mail Manager, puoi utilizzare la procedura guidata Guida introduttiva a Mail Manager nella console Amazon SES, dove potrai creare un endpoint di ingresso e configurarlo con una policy sul traffico e un set di regole.

Un endpoint di ingresso è il primo elemento costitutivo della configurazione di Mail Manager: è un componente chiave dell'infrastruttura che utilizza:

- Criteri sul traffico: una politica sul traffico contiene dichiarazioni politiche definite dall'utente per ordinare la posta in arrivo autorizzando o bloccando tipi specifici di e-mail quando vengono soddisfatte le condizioni dell'informativa.
- Set di regole: un set di regole contiene le regole che definisci per eseguire azioni sull'e-mail a cui autorizzi l'invio quando vengono soddisfatte le condizioni della regola.

Tuttavia, parte della creazione di un endpoint di ingresso consiste nel selezionare una politica di traffico e un set di regole già creati e quindi assegnarli all'endpoint di ingresso. I passaggi della procedura seguente illustreranno l'ordine corretto di configurazione del primo endpoint di ingresso.

Guida introduttiva a Mail Manager tramite la console SES

La procedura seguente mostra come iniziare a usare Mail Manager utilizzando la console SES.

Per iniziare a usare Mail Manager utilizzando la console Amazon SES

1. Accedi AWS Management Console e apri la console Amazon SES all'indirizzo https://console.aws.amazon.com/ses/.
2. Nel pannello di navigazione a sinistra, scegli Mail Manager e seleziona uno dei pulsanti Inizia a usare Mail Manager nella pagina di panoramica di Mail Manager.
3. Nella pagina Inizia a configurare, seleziona Crea una politica del traffico nella scheda Crea una politica del traffico.

    a. Completa il flusso di lavoro nella pagina Crea una politica sul traffico. Se hai bisogno di ulteriori informazioni, consultathe section called “Creazione di politiche e dichiarazioni politiche sul traffico (console)”.

    b. Dopo aver creato la prima politica sul traffico e le relative dichiarazioni, utilizza il pulsante Indietro del browser per tornare alla pagina di configurazione o seleziona Inizia la configurazione in Mail Manager nel pannello di navigazione a sinistra.
4. Nella pagina Inizia a configurare, seleziona Crea set di regole nella scheda Crea un set di regole.

    a. Completa il flusso di lavoro nella pagina Crea un set di regole. Se hai bisogno di ulteriori informazioni, consultathe section called “Creazione di set di regole e regole (console)”.

    b. Dopo aver creato il primo set di regole e le regole, usa il pulsante Indietro del browser per tornare alla pagina di configurazione o seleziona Inizia la configurazione in Mail Manager nel pannello di navigazione a sinistra.
5. Ora che hai creato la tua prima politica sul traffico e il primo set di regole, sarai in grado di creare il tuo primo endpoint di ingresso. Nella pagina Inizia la configurazione, seleziona Crea endpoint di ingresso nella scheda Crea un endpoint di ingresso.

    - Parte del flusso di lavoro nella pagina dell'endpoint di ingresso della posta elettronica consisterà nell'assegnare la politica sul traffico e il set di regole appena creati all'endpoint di ingresso. Se hai bisogno di ulteriori informazioni, consulta. the section called “Creazione di un endpoint di ingresso (console)”

Dopo la creazione del primo endpoint di ingresso, è possibile iniziare a utilizzare Mail Manager e utilizzare le sue altre funzionalità, come i relè SMTP e l'archiviazione delle e-mail. È inoltre possibile creare endpoint di ingresso aggiuntivi con politiche di traffico e set di regole unici per personalizzare ulteriormente la gestione di tutte le e-mail in arrivo.

Endpoint di ingresso

Un endpoint di ingresso è il componente chiave dell'infrastruttura di Mail Manager che riceve, indirizza e gestisce le e-mail utilizzando politiche e regole configurate per determinare quali e-mail devono essere rifiutate, quali devono essere consentite e su quali agire.

Ogni endpoint di ingresso ha una propria politica sul traffico per determinare quali e-mail bloccare o consentire e un proprio set di regole per eseguire azioni sull'e-mail a cui si consente l'invio; pertanto, creando più endpoint di ingresso, è possibile delegare ciascuno di essi alla gestione e al routing di tipi specifici di e-mail. Questo livello di granularità ti aiuterà a creare un sistema di gestione della posta elettronica personalizzato in base alle tue esigenze aziendali.

Flusso di lavoro prerequisito per creare un endpoint di ingresso

Al momento della creazione dell'endpoint di ingresso, è necessario assegnargli una politica sul traffico e un set di regole già creati. Pertanto, il flusso di lavoro per la creazione di un endpoint di ingresso deve essere nel seguente ordine:

1. Inizia creando una politica sul traffico per determinare l'e-mail che desideri bloccare o consentire. Per informazioni dettagliate, vedi the section called “Creazione di politiche e dichiarazioni politiche sul traffico (console)”.
2. Quindi, crea un set di regole per eseguire azioni sull'e-mail a cui autorizzi l'invio. Per informazioni dettagliate, vedi the section called “Creazione di set di regole e regole (console)”.
3. Infine, crea il tuo endpoint di ingresso e assegnagli la politica sul traffico e il set di regole che hai appena creato o qualsiasi altro che hai creato in precedenza.

Una volta creato l'endpoint di ingresso, devi configurarlo con l'ambiente che stai utilizzando per ricevere e-mail, che si tratti della configurazione di un client SMTP locale o di un host di dominio DNS basato sul web. Questo è discusso di seguito in. the section called “Configurazione dell'ambiente ”

Configurazione dell'ambiente per l'utilizzo di un endpoint di ingresso

Utilizzo del record «A»

Al momento della creazione di un endpoint di ingresso, verrà generato un record «A» per l'endpoint e il relativo valore verrà visualizzato nella schermata di riepilogo dell'endpoint di ingresso nella console SES. Il modo in cui utilizzate il valore di questo record dipende dal tipo di endpoint creato e dal vostro caso d'uso:

- Endpoint aperto: la posta inviata al tuo dominio verrà risolta direttamente sull'endpoint di ingresso, senza bisogno di autenticazione.
  - Copia e incolla il valore del record «A» direttamente nella configurazione SMTP di un client SMTP locale o in un record MX per il tuo dominio nella tua configurazione DNS.
- Endpoint autenticato: la posta inviata al tuo dominio deve provenire da mittenti autorizzati con cui hai condiviso le tue credenziali SMTP, come i server di posta elettronica locali.
  - Copia e incolla il valore del record «A» direttamente nella configurazione SMTP di un client SMTP locale, oltre al nome utente e alla password.

Se utilizzi un record MX nella tua configurazione, tieni presente che, sebbene ogni provider DNS abbia procedure e interfacce diverse per la configurazione dei record, le informazioni chiave da inserire nelle impostazioni DNS sono elencate nell'esempio seguente:

Tutte le e-mail inviate a recipient@marketing.example.com andranno al tuo endpoint di ingresso perché hai inserito il record «A» dell'endpoint di ingresso come valore per un record MX nelle impostazioni DNS del tuo dominio:

- Dominio: `marketing.example.com`
- Valore del record MX: `890123abcdef.ghijk.mail-manager-smtp.amazonaws.com` (è il valore del record «A» copiato dall'endpoint di ingresso).
- Priorità — `10`

La procedura riportata nella sezione successiva illustrerà come creare un endpoint di ingresso nella console SES.

Creazione di un endpoint di ingresso nella console SES

La procedura seguente mostra come utilizzare la pagina degli endpoint Ingress nella console SES per creare endpoint di ingresso e gestire quelli già creati.

Per creare e gestire gli endpoint di ingresso utilizzando la console

1. Accedi AWS Management Console e apri la console Amazon SES all'indirizzo https://console.aws.amazon.com/ses/.
2. Nel pannello di navigazione a sinistra, scegli Ingress endpoints in Mail Manager.
3. Nella pagina Ingress endpoint, seleziona Crea endpoint in ingresso.
4. Nella pagina Crea un nuovo endpoint di ingresso, inserisci un nome univoco per il tuo endpoint di ingresso.
5. Scegli se sarà un endpoint aperto o autenticato.

   - Se scegli Autenticato, seleziona Password SMTP e inserisci una password oppure Segreto e seleziona uno dei tuoi segreti da Secret ARN. Se si seleziona un segreto creato in precedenza, questo deve contenere le politiche indicate nei passaggi seguenti per la creazione di un nuovo segreto.
   - Hai la possibilità di creare un nuovo segreto scegliendo Crea nuovo: si aprirà la AWS Secrets Manager console dove potrai continuare a creare una nuova chiave:

   a. Scegli Altro tipo di segreto in Tipo segreto.
   b. Nella coppia chiave/valore, inserite `password` la chiave e la password effettiva per il valore.

      > **Note**
      >
      > Per Key, devi solo inserire `password` (qualsiasi altra operazione impedirà l'autenticazione).

   c. Seleziona Aggiungi nuova chiave per creare una chiave gestita dal cliente (CMK) KMS nella chiave di crittografia: la AWS KMS console si aprirà.
   d. Scegli Crea chiave nella pagina Chiavi gestite dal cliente.
   e. Mantieni i valori predefiniti nella pagina Configura chiave e seleziona Avanti.
   f. Inserisci un nome per la tua chiave in Alias (facoltativamente, puoi aggiungere una descrizione e un tag), seguito da Avanti.
   g. Seleziona gli utenti (diversi da te) o i ruoli a cui desideri consentire l'amministrazione della chiave in Amministratori chiave seguito da Next.
   h. Seleziona tutti gli utenti (diversi da te) o i ruoli a cui desideri consentire l'uso della chiave in Utenti chiave seguito da Next.

i. Copiala e incollala Politica KMS CMK nell'editor di testo JSON di Key policy a `"statement"` livello aggiungendola come istruzione aggiuntiva separata da una virgola. Sostituisci la regione e il numero di conto con i tuoi.

j. Scegli Fine.

k. Seleziona la scheda del browser in cui hai aperto AWS Secrets Manager Memorizza una nuova pagina segreta e seleziona l'icona di aggiornamento (freccia circolare) accanto al campo Chiave di crittografia, quindi fai clic all'interno del campo e seleziona la chiave appena creata.

l. Inserisci un nome nel campo Nome segreto nella pagina Configura segreto.

m. Seleziona Modifica autorizzazioni in Autorizzazioni per le risorse.

n. Copiali e incollali Politica delle risorse segrete nell'editor di testo JSON Resource permissions e sostituisci la regione e il numero di account con i tuoi. (Assicurati di eliminare qualsiasi codice di esempio nell'editor.)

o. Scegli Salva seguito da Avanti.

p. Se lo desideri, configura la rotazione seguita da Avanti.

q. Controlla e archivia il tuo nuovo segreto selezionando Store.

r. Seleziona la scheda del browser in cui è aperta la pagina SES Create new ingress endpoint e scegli Aggiorna elenco, quindi seleziona il segreto appena creato in Secret ARN.

6. Seleziona una politica sul traffico per determinare l'e-mail che desideri bloccare o consentire.
7. Seleziona un set di regole contenente le azioni relative alle regole che desideri eseguire sull'e-mail a cui autorizzi l'invio.
8. Seleziona Crea endpoint di ingresso.
9. In generale, verrà visualizzato «Provisioning» durante la creazione dell'endpoint di ingresso: aggiorna la pagina finché non viene visualizzato «Attivo» e il campo ARecord contiene un valore. Copia il valore del record «A» e incollalo nella configurazione DNS o nel client SMTP come descritto in. Configurazione dell'ambiente
10. Puoi visualizzare e gestire gli endpoint di ingresso che hai già creato dalla pagina degli endpoint di Ingress. Se c'è un endpoint di ingresso che desideri rimuovere, seleziona il pulsante di opzione corrispondente seguito da Elimina.
11. Per modificare un dispositivo di ingresso, selezionane il nome per aprire la pagina di riepilogo:

    - È possibile modificare lo stato attivo dell'endpoint selezionando Modifica in Dettagli generali, seguito da Salva modifiche.

- Puoi selezionare un set di regole o una politica di traffico diversi scegliendo Modifica in Set di regole o Politica sul traffico, seguito da Salva modifiche.

Politiche e dichiarazioni politiche sul traffico

Una politica sul traffico è un contenitore di dichiarazioni di policy assegnate a un endpoint di ingresso in modo che possa ordinare la posta in arrivo autorizzando o bloccando tipi specifici di e-mail quando vengono soddisfatte le condizioni delle dichiarazioni politiche. Una politica del traffico può essere utilizzata da più endpoint di ingresso.

> **Tip**
>
> È possibile pensare a una politica sul traffico come a un «set di filtri» e a una dichiarazione politica come a un «filtro». La politica sul traffico (set di filtri) contiene criteri (filtri) che utilizzi per filtrare la posta in arrivo.

Quando crei una politica sul traffico, hai la possibilità di impostare una dimensione massima dei messaggi (in byte). Quando un messaggio supera tale dimensione, viene immediatamente scartato. Se impostato, questo funge da filtro di «primo passaggio». Successivamente, imposti l'azione predefinita per consentire o bloccare le e-mail che non rientrano nelle condizioni delle tue politiche: considerala un'azione «catch all» per la politica sul traffico.

Le dichiarazioni politiche vengono inoltre create con un'azione di autorizzazione o di blocco che viene intrapresa quando vengono soddisfatte le condizioni delle istruzioni. Le condizioni vengono create selezionando un protocollo di posta elettronica e un operatore condizionale per un valore immesso che deve corrispondere al messaggio in arrivo prima che l'informativa sulla politica lo consenta o lo blocchi. Ogni dichiarazione politica può avere più condizioni.

Una politica sul traffico può contenere più istruzioni politiche ed eseguirle in un ordine basato sulla gerarchia implicita di come valuta la posta elettronica:

- Dimensione massima del messaggio: se questo parametro facoltativo è impostato, qualsiasi messaggio superiore a tale dimensione viene immediatamente scartato, ignorando le istruzioni relative alle politiche.
- Dichiarazioni politiche che bloccano: queste istruzioni vengono valutate per prime e bloccano qualsiasi messaggio che soddisfi le condizioni dell'istruzione.

- Dichiarazioni politiche che lo consentono: queste dichiarazioni vengono valutate successivamente e consentono qualsiasi messaggio che soddisfi le condizioni dell'informativa.
- Azione predefinita della politica sul traffico: i restanti messaggi che non rientrano nelle dichiarazioni politiche sono consentiti o bloccati in base alla definizione di questo parametro.

Una politica sul traffico è una risorsa indipendente che può essere utilizzata da più di un endpoint di ingresso, ma le dichiarazioni politiche appartengono esclusivamente alla politica sul traffico in cui sono state create. Pertanto, è necessario innanzitutto creare una politica sul traffico o modificarne una esistente prima di poter creare dichiarazioni politiche per valutare l'e-mail che arriva all'endpoint di ingresso.

La procedura nella sezione successiva spiega come creare politiche sul traffico e le relative dichiarazioni politiche nella console SES.

Creazione di politiche e dichiarazioni politiche sul traffico nella console SES

La procedura seguente mostra come utilizzare la pagina delle politiche di traffico nella console SES per creare politiche di traffico e le relative dichiarazioni politiche e gestire quelle già create.

Per creare e gestire le politiche sul traffico e le dichiarazioni politiche utilizzando la console

1. Accedi AWS Management Console e apri la console Amazon SES all'indirizzo https://console.aws.amazon.com/ses/.
2. Nel pannello di navigazione a sinistra, scegli Politiche sul traffico in Mail Manager.
3. Nella pagina Politiche sul traffico, seleziona Crea politica sul traffico.
4. Nella pagina Crea una politica sul traffico, inserisci un nome univoco per la tua politica sul traffico.
5. (Facoltativo) Se desideri eliminare i messaggi che superano una certa dimensione, inserisci un valore in byte nel campo Dimensione massima del messaggio.
6. Nel campo Azione predefinita, scegli se la politica sul traffico deve consentire o rifiutare (bloccare) i messaggi che non rientrano nelle condizioni delle tue dichiarazioni politiche (non sono regolati da).
7. Seleziona Aggiungi nuova dichiarazione politica per creare una dichiarazione per la tua politica sul traffico.
8. Scegli Consenti o Nega (blocca) per l'azione da intraprendere quando le condizioni dell'informativa sono soddisfatte.

9. Crea una condizione selezionando un protocollo e-mail e un operatore condizionale per il valore inserito. Seleziona Aggiungi nuova condizione se desideri aggiungere altre condizioni a questa dichiarazione politica. Per ulteriori informazioni su una proprietà condizionale e sui relativi operatori e valori validi, consulta il riferimento alle condizioni della dichiarazione politica.

    - Se sei abbonato a un componente aggiuntivo per la posta elettronica, potrai selezionarlo qui come protocollo di posta elettronica.

10. Se desideri aggiungere altre dichiarazioni e condizioni relative alle politiche, ripeti i passaggi da 7 a 9 precedenti.
11. Quando hai finito di creare le dichiarazioni politiche e le relative condizioni, seleziona Crea politica sul traffico.
12. Puoi visualizzare e gestire le politiche sul traffico che hai già creato dalla pagina Politiche sul traffico. Se c'è una politica sul traffico che desideri rimuovere, seleziona il relativo pulsante di opzione seguito da Elimina.
13. Per modificare le proprietà di una politica del traffico o una delle sue dichiarazioni politiche, selezionane il nome per aprire la pagina di panoramica, da qui seleziona Modifica.
14. Nei dettagli delle politiche sul traffico, puoi modificare la dimensione massima dei messaggi e l'azione predefinita.
15. In qualsiasi contenitore di istruzioni Policy, è possibile modificare la proprietà allow/deny e modificare qualsiasi condizione. È inoltre possibile rimuovere le dichiarazioni e le condizioni relative alle politiche e aggiungerne di nuove.
16. Quando hai finito con tutte le modifiche, salva le modifiche selezionando Salva modifiche.

Riferimento per le condizioni della dichiarazione politica

Condizioni della dichiarazione politica

La seguente tabella di riferimento elenca tutti i protocolli di dichiarazione politica disponibili per creare una condizione di dichiarazione politica. Selezionando il tipo di espressione di un protocollo si accede alla relativa pagina di riferimento nel SES Mail Manager API Reference, che elenca tutti gli operatori disponibili e i valori validi per quel protocollo.

Condizioni della dichiarazione politica: protocolli, operatori e valori

Protocollo	Tipo di espressione
Indirizzo del destinatario	Operatori e valori validi per le espressioni di stringa
Intervallo IP del mittente	Operatori e valori validi per le espressioni IP
Versione del protocollo TLS	Operatori e valori validi per le espressioni del protocollo TLS
Abusix Mail Intelligence (se sottoscritto) Lista dei domini bloccati di Spamhaus (se sottoscritto)	Operatori e valori validi per le espressioni booleane

Set di regole e regole

I set di regole sono contenitori di regole da assegnare a un endpoint di ingresso in modo che possa eseguire azioni sulle e-mail consentite dalla politica di traffico dell'endpoint di ingresso. Un set di regole può essere utilizzato da più endpoint di ingresso.

Le regole indicano all'endpoint di ingresso come gestire la posta elettronica in arrivo eseguendo le azioni definite nella regola quando i messaggi soddisfano le condizioni della regola. Ogni regola può avere più condizioni e azioni. Le regole create all'interno di un set di regole vengono eseguite nell'ordine specificato all'interno del set di regole.

Le condizioni della regola vengono create selezionando una proprietà di posta elettronica e un operatore condizionale per un valore immesso a cui deve corrispondere il messaggio prima che la regola esegua le proprie azioni: si definiscono le azioni da intraprendere e il relativo ordine di esecuzione.

Per una maggiore granularità, le regole possono contenere anche eccezioni definite in modo simile alle condizioni, ma in questo caso si definisce una condizione che il messaggio non deve soddisfare. Le condizioni e le eccezioni funzionano in modo indipendente: puoi creare una regola con solo eccezioni, se lo desideri, oltre a una combinazione di condizioni ed eccezioni.

A causa della grande granularità del modo in cui le regole possono essere definite all'interno di un set di regole, viene fornito il seguente elenco per illustrare la relazione tra i componenti del set di regole:

- I set di regole contengono:
  - Regole: è possibile definire l'ordine in cui le regole vengono eseguite all'interno del set di regole.

    Le regole contengono:
    - Condizioni: la regola si applica se il messaggio corrisponde alla valutazione delle condizioni; e se la regola ha delle eccezioni, vedi sotto.
    - Eccezioni: la regola si applica se il messaggio non corrisponde alla valutazione delle eccezioni; e se la regola ha delle condizioni, vedi sopra.
    - Azioni: le azioni vengono attivate quando si applica la regola: tutte le condizioni soddisfano e nessuna delle eccezioni.

      È possibile definire l'ordine in cui le azioni vengono eseguite all'interno della regola.

Poiché ogni regola può avere più condizioni, eccezioni e azioni e il fatto che è possibile definire l'ordine di esecuzione delle regole e delle azioni, ciò consente di creare una soluzione di gestione della posta elettronica molto personalizzata e automatizzata, adattata alle specifiche esigenze aziendali.

Un set di regole è una risorsa indipendente che può essere utilizzata da più di un endpoint di ingresso, ma le regole appartengono esclusivamente al set di regole in cui sono state create. Pertanto, è necessario innanzitutto creare un set di regole o modificarne uno esistente prima di poter creare regole per agire sull'e-mail che arriva all'endpoint di ingresso.

La procedura riportata nella sezione successiva vi guiderà nella creazione dei set di regole e delle relative regole nella console SES.

Creazione di set di regole e regole nella console SES

La procedura seguente mostra come utilizzare la pagina Set di regole nella console SES per creare set di regole e le relative regole e gestire quelle già create.

Per creare e gestire set di regole e regole utilizzando la console

1. Accedi AWS Management Console e apri la console Amazon SES all'indirizzo https://console.aws.amazon.com/ses/.
2. Nel pannello di navigazione a sinistra, scegli Set di regole in Mail Manager.
3. Nella pagina Set di regole, scegli Crea set di regole e inserisci un nome univoco per il set di regole.

4. Nella pagina di panoramica del set di regole, seleziona Modifica, quindi seleziona Crea nuova regola nella pagina di modifica.
5. Nella barra laterale dei dettagli della regola, inserisci un nome univoco per la regola.
6. Seleziona Aggiungi nuova condizione per creare una condizione a cui il messaggio deve soddisfare; oppure seleziona la casella ECCETTO in caso di: seguita da Aggiungi nuova eccezione per creare una condizione a cui il messaggio non deve corrispondere.
7. Crea la condizione o l'eccezione selezionando una proprietà di posta elettronica e un operatore condizionale per il valore immesso. Seleziona Aggiungi nuova condizione o Aggiungi nuova eccezione se desideri aggiungere altre condizioni o eccezioni a questa regola. Per ulteriori informazioni su una proprietà di condizione e sui relativi operatori e valori validi, consulta il riferimento alle condizioni della regola.

   - Se sei abbonato a un componente aggiuntivo e-mail, potrai selezionarlo qui come proprietà e-mail.
8. Seleziona Aggiungi nuova azione per definire l'azione da intraprendere quando le condizioni della regola sono soddisfatte e/o le eccezioni non sono soddisfatte. Per aggiungere altre azioni da intraprendere, seleziona Aggiungi nuova azione. Per ulteriori informazioni sulle azioni e sui relativi parametri, consulta il riferimento alle azioni delle regole.

   - Per eseguire le azioni delle regole Scrivi a S3, Consegna alla casella di posta e Invia a Internet, devi averle Politiche di azione sulle regole abilitate per il tuo account; in caso contrario, l'azione della regola avrà esito negativo.
   - Quando crei due o più azioni, vengono visualizzate le frecce su/giù per impostare l'ordine di esecuzione.
9. Dopo aver creato le condizioni, le eccezioni e le azioni per la regola, la salvi nel relativo set di regole scegliendo Salva set di regole situato nel pannello Modifica set di regole a sinistra.
10. Se desideri aggiungere altre regole al set di regole, ripeti i passaggi da 4 a 9 precedenti.

    - Quando si creano due o più regole, nella colonna Riordina del set di regole vengono visualizzate le frecce su/giù in modo da poter impostare l'ordine di esecuzione.
11. È possibile visualizzare e gestire i set di regole già creati dalla pagina Set di regole. Se c'è un set di regole che desideri rimuovere, seleziona il relativo pulsante di opzione seguito da Elimina.
12. Per modificare un set di regole, selezionane il nome per aprirne la pagina di panoramica, da qui seleziona Modifica dove puoi riordinare l'esecuzione delle relative regole, aggiungere altre regole scegliendo Crea nuova regola o eliminare una regola selezionando il relativo pulsante di opzione seguito da Elimina.

13. Per modificare una regola, seleziona il relativo pulsante di opzione. In uno qualsiasi dei contenitori della barra laterale dei dettagli della regola, puoi modificare qualsiasi condizione o eccezione e modificare o riordinare qualsiasi azione. Puoi anche rimuovere condizioni, eccezioni e azioni, nonché aggiungerne di nuove.
14. Quando hai finito con tutte le modifiche, salva le modifiche selezionando Salva set di regole nel pannello Modifica set di regole a sinistra.

Riferimento per le condizioni e le azioni delle regole

Condizioni delle regole

La seguente tabella di riferimento elenca tutte le proprietà delle regole disponibili per creare una condizione (o eccezione) di una regola e sono classificate in base al tipo di espressione. Le proprietà delle regole che condividono lo stesso tipo di espressione condividono anche gli stessi operatori e valori. Selezionando il tipo di espressione di una proprietà si accede alla relativa pagina di riferimento in SES Mail Manager API Reference, che elenca tutti gli operatori disponibili e i valori validi per quella proprietà.

Condizioni della regola: proprietà, operatori e valori

Proprietà	Tipo di espressione
Indirizzo del mittente	Operatori e valori validi per le espressioni di stringa
All'indirizzo	
Indirizzo CC	
Posta da	
Indirizzo del destinatario	
Subject	
Aiuto	
Intervallo IP	Operatori e valori validi per le espressioni IP
Dimensione massima del messaggio	Operatori e valori validi per le espressioni numeriche

Proprietà	Tipo di espressione
DKIM SPF Trend Micro Virus Scanning (se abbonato)	Operatori e valori validi per le espressioni di verdetto
TLS TLS avvolto Leggi la ricevuta	Operatori e valori validi per le espressioni booleane
Politica DMARC	Operatori e valori validi per le espressioni DMARC

Azioni relative alle regole

La seguente tabella di riferimento elenca tutte le azioni che è possibile intraprendere quando le condizioni di una regola sono soddisfatte o le relative eccezioni non sono soddisfatte. Selezionando un'azione, verrai indirizzato alla pagina di riferimento dell'azione in SES Mail Manager API Reference, che elenca i parametri e i relativi formati per l'azione. La tabella utilizza i nomi delle azioni adottati nella console di Mail Manager: i nomi delle API possono differire leggermente.

> **Note**
>
> In alcuni riferimenti alle API, ci sarà un *`ActionFailurePolicy`* parametro che può essere impostato su Continue o Drop se l'azione fallisce, questo vale solo quando si utilizza l'API; quando si utilizza la console, *`ActionFailurePolicy`* è stato impostato sul valore predefinito Continue.

Azioni delle regole: azioni e parametri

Azioni e relativi parametri	Descrizione
Scrivi su S3	Scrive il contenuto MIME dell'e-mail in un bucket S3.

Azioni e relativi parametri	Descrizione
Azione di inoltro SMTP	Inoltra l'e-mail tramite SMTP a un altro server SMTP specifico.
Azione di archiviazione	Archivia l'e-mail inviandola a un archivio Amazon SES.
Aggiungi un'intestazione	Aggiunge un'intestazione personalizzata all'e-mail ricevuta.
I destinatari delle e-mail riscrivono	Sostituisce i destinatari della busta di posta elettronica con l'elenco di destinatari fornito. Se la condizione di questa azione si applica solo a un sottoinsieme di destinatari, vengono sostituiti solo tali destinatari.
Consegna alla casella di posta	Invia l'e-mail a una WorkMail casella di posta Amazon.
Invia a Internet	Utilizza SES per inviare l'e-mail ai destinatari presenti nell'elenco dei destinatari dell'e-mail.
Eliminare l'azione	Per le e-mail con più destinatari, se questa azione si applica a uno o più (ma non a tutti) di tali destinatari, questi verranno eliminati dall'elenco dei destinatari dell'e-mail e l'elaborazione continua delle regole verrà applicata ai destinatari rimanenti. Se questa azione si applica a tutti i destinatari, l'elaborazione delle regole si interrompe poiché tutti i destinatari vengono eliminati dall'elenco dei destinatari e non riceveranno l'e-mail.

Relè SMTP

Poiché Mail Manager viene distribuito tra l'ambiente di posta elettronica (ad esempio Microsoft 365, Google Workspace o On-Premise Exchange) e Internet, Mail Manager utilizza i relè SMTP

per indirizzare le e-mail in arrivo elaborate da Mail Manager all'ambiente di posta elettronica dell'utente. Può anche instradare le e-mail in uscita verso un'altra infrastruttura di posta elettronica, ad esempio un altro server Exchange o un gateway di posta elettronica di terze parti, prima di inviarle ai destinatari finali.

Un relay SMTP è un componente fondamentale dell'infrastruttura di posta elettronica, responsabile del routing efficiente delle e-mail tra i server quando indicato da un'azione di regola definita in un set di regole.

In particolare, un relay SMTP può reindirizzare la posta elettronica in arrivo tra SES Mail Manager e un'infrastruttura di posta elettronica esterna come Exchange, gateway di posta elettronica locali o di terze parti e altri. Le e-mail in arrivo verso un dispositivo di ingresso verranno elaborate in base a una regola che indirizzerà l'e-mail specificata al relay SMTP designato, che a sua volta la trasmetterà all'infrastruttura di posta elettronica esterna definita nel relay SMTP.

Quando l'endpoint di ingresso riceve e-mail, utilizza una politica sul traffico per determinare quali e-mail bloccare o consentire. L'e-mail che autorizzi passa a un set di regole che applica regole condizionali per eseguire le azioni che hai definito per tipi specifici di e-mail. Una delle azioni che puoi definire è l'azione SMTPrelay: se selezioni questa azione, l'e-mail verrà passata al server SMTP esterno definito nel relay SMTP.

Ad esempio, è possibile utilizzare l'azione SMTPrelay per inviare e-mail dall'endpoint di ingresso al server Microsoft Exchange locale. È consigliabile configurare il server Exchange in modo che disponga di un endpoint SMTP pubblico a cui è possibile accedere solo utilizzando determinate credenziali. Quando si crea il relè SMTP, si inseriscono il nome del server, la porta e le credenziali del server Exchange e si assegna al relay SMTP un nome univoco, ad esempio "». RelayToMyExchangeServer Quindi, crei una regola nel set di regole del tuo endpoint di ingresso che dice: «Quando l'indirizzo From contiene 'gmail.com', quindi esegui l'azione SMTPrelay utilizzando il relè SMTP chiamato». RelayToMyExchangeServer

Ora, quando l'e-mail da gmail.com arriva all'endpoint di ingresso, la regola attiverà l'azione SMTPrelay e contatterà il server Exchange utilizzando le credenziali fornite durante la creazione del relay SMTP e consegnerà l'e-mail al server Exchange. Pertanto, le e-mail ricevute da gmail.com vengono inoltrate al server Exchange.

È necessario innanzitutto creare un relè SMTP prima di poterlo designare in un'azione di regola. La procedura riportata nella sezione successiva illustrerà come creare un relay SMTP nella console SES.

Creazione di un relè SMTP nella console SES

La procedura seguente mostra come utilizzare la pagina dei relè SMTP nella console SES per creare relè SMTP e gestire quelli già creati.

Per creare e gestire i relè SMTP utilizzando la console

1. Accedi AWS Management Console e apri la console Amazon SES all'indirizzo https://console.aws.amazon.com/ses/.
2. Nel pannello di navigazione a sinistra, scegli Relay SMTP in Mail Manager.
3. Nella pagina dei relè SMTP, seleziona Crea relè SMTP.
4. Nella pagina Crea relè SMTP, inserisci un nome univoco per il tuo relay SMTP.
5. A seconda che vogliate configurare un relè SMTP in entrata (non autenticato) o in uscita (autenticato), seguite le rispettive istruzioni:

   Inbound

   Per configurare un relè SMTP in entrata

   1. Quando il relay SMTP viene utilizzato come gateway in entrata per indirizzare le e-mail in arrivo elaborate da Mail Manager verso l'ambiente di posta elettronica esterno, è necessario prima configurare l'ambiente di hosting della posta elettronica. Sebbene ogni provider di hosting di posta elettronica abbia una propria interfaccia grafica e un flusso di lavoro di configurazione unici, i principi per configurarlo per funzionare con i gateway in entrata, come il relè SMTP di Mail Manager, saranno simili.

      A scopo di illustrazione, abbiamo fornito esempi di come configurare Google Workspaces e Microsoft Office 365 per utilizzare il relè SMTP come gateway in entrata nelle seguenti sezioni:

      - Configurazione di Google Workspaces
      - Configurazione di Microsoft Office 365

      Attualmente SES supporta solo relè SMTP in entrata (non autenticati) per Google Workspaces e Microsoft Office 365.

> **Note**
>
> Assicurati che i domini delle destinazioni dei destinatari previsti siano identità di dominio verificate da SES. Ad esempio, se desideri recapitare e-mail ai destinatari abc@example.com e support@acme.com, entrambi i domini example.com e acme.com devono essere verificati in SES. Se il dominio di un destinatario non è verificato, SES non tenterà di recapitare l'e-mail al server SMTP pubblico. Per ulteriori informazioni, consulta the section called “Creazione e verifica delle identità”.

2. Dopo aver configurato Google Workspaces o Microsoft Office 365 per funzionare con i gateway in entrata, inserisci il nome host del server SMTP pubblico con i valori seguenti relativi al tuo provider:

   - Google Workspaces: `aspmx.l.google.com`
   - Microsoft Office 365: `<your_domain>.mail.protection.outlook.com`

     Sostituisci i punti con «-» nel tuo nome di dominio. Ad esempio, se il tuo dominio è acme.com, devi inserire `acme-com.mail.protection.outlook.com`

3. Immettete il numero di porta 25 per il server SMTP pubblico.
4. Lascia vuota la sezione Autenticazione (non selezionare o creare un ARN segreto).

Outbound

Per configurare un relè SMTP in uscita

1. Inserisci il nome host del server SMTP pubblico a cui desideri connettere il relè.
2. Immettete il numero di porta per il server SMTP pubblico.
3. Configura l'autenticazione per il tuo server SMTP selezionando uno dei tuoi segreti da Secret ARN. Se si seleziona un segreto creato in precedenza, questo deve contenere le politiche indicate nei passaggi seguenti per la creazione di un nuovo segreto.

   - Hai la possibilità di creare un nuovo segreto scegliendo Crea nuovo: si aprirà la AWS Secrets Manager console dove potrai continuare a creare una nuova chiave:

     a. Scegli Altro tipo di segreto in Tipo segreto.

b. Inserisci le seguenti chiavi e valori nelle coppie chiave/valore:

Chiave	value
`username`	mio_nome utente
`password`	mia_password

> **Note**
>
> Per entrambe le chiavi, devi solo inserire `username` e fare `password` come mostrato (qualsiasi altra operazione impedirà l'autenticazione). Per i valori, inserite rispettivamente il vostro nome utente e la vostra password.

c. Seleziona Aggiungi nuova chiave per creare una chiave gestita dal cliente (CMK) KMS nella chiave di crittografia: la AWS KMS console si aprirà.

d. Scegli Crea chiave nella pagina Chiavi gestite dal cliente.

e. Mantieni i valori predefiniti nella pagina Configura chiave e seleziona Avanti.

f. Inserisci un nome per la tua chiave in Alias (facoltativamente, puoi aggiungere una descrizione e un tag), seguito da Avanti.

g. Seleziona tutti gli utenti (diversi da te) o i ruoli a cui desideri consentire l'amministrazione della chiave in Amministratori chiave seguito da Next.

h. Seleziona tutti gli utenti (diversi da te) o i ruoli a cui desideri consentire l'uso della chiave in Utenti chiave seguito da Next.

i. Copiala e incollala Politica KMS CMK nell'editor di testo JSON di Key policy a `"statement"` livello aggiungendola come istruzione aggiuntiva separata da una virgola. Sostituisci la regione e il numero di conto con i tuoi.

j. Scegli Fine.

k. Seleziona la scheda del browser in cui hai aperto AWS Secrets Manager Memorizza una nuova pagina segreta e seleziona l'icona di aggiornamento (freccia circolare) accanto al campo Chiave di crittografia, quindi fai clic all'interno del campo e seleziona la chiave appena creata.

l. Inserisci un nome nel campo Nome segreto nella pagina Configura segreto.

m. Seleziona Modifica autorizzazioni in Autorizzazioni per le risorse.

n. Copiali e incollali Politica delle risorse segrete nell'editor di testo JSON Resource permissions e sostituisci la regione e il numero di account con i tuoi. (Assicurati di eliminare qualsiasi codice di esempio nell'editor.)

o. Scegli Salva seguito da Avanti.

p. Se lo desideri, configura la rotazione seguita da Avanti.

q. Controlla e archivia il tuo nuovo segreto selezionando Store.

r. Seleziona la scheda del browser in cui è aperta la pagina SES Create new ingress endpoint e scegli Aggiorna elenco, quindi seleziona il segreto appena creato in Secret ARN.

6. Seleziona Crea relè SMTP.
7. Puoi visualizzare e gestire i relè SMTP che hai già creato dalla pagina dei relè SMTP. Se c'è un relè SMTP che desideri rimuovere, seleziona il relativo pulsante di opzione seguito da Elimina.
8. Per modificare un relè SMTP, selezionane il nome. Nella pagina dei dettagli, è possibile modificare il nome del relè, il nome, la porta e le credenziali di accesso del server SMTP esterno selezionando il pulsante Modifica o Aggiorna corrispondente seguito da Salva modifiche.

Configurazione di Google Workspaces per l'inoltro SMTP in entrata (non autenticato)

Il seguente esempio dettagliato mostra come configurare Google Workspaces per l'utilizzo di un relay SMTP in entrata (non autenticato) di Mail Manager.

Prerequisiti

- Accesso alla console di amministrazione Google (console di amministrazione Google > App > Google Workspace > Gmail).
- Accesso al nameserver di dominio che ospita i record MX per i domini che verranno utilizzati per la configurazione di Mail Manager.

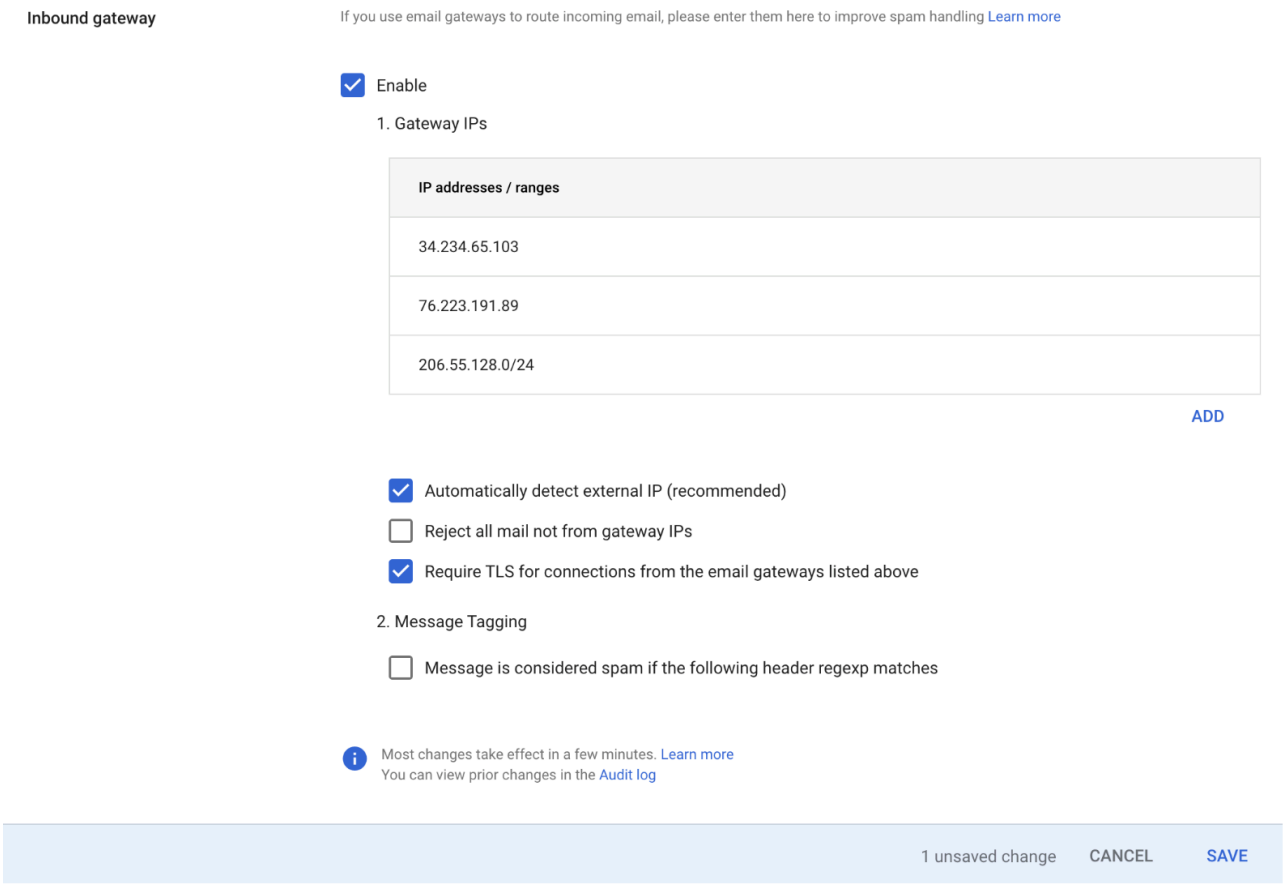
Per configurare Google Workspaces in modo che funzioni con un relè SMTP in entrata

- Aggiungi gli indirizzi IP di Mail Manager alla configurazione del gateway in entrata

  a. Nella console di amministrazione di Google, vai su App > Google Workspace > Gmail.

  b. Seleziona Spam, phishing e malware, quindi vai alla configurazione del gateway in entrata.

c. Abilita il gateway in entrata e configuralo con i seguenti dettagli:



- In Gateway IPs, seleziona Aggiungi e aggiungi gli IP degli endpoint di ingresso specifici per la tua regione dalla seguente tabella:

Regione	Intervallo IP
UE-West-1/DUB	206.55.133,0/24
UE-centrale-1/FRA	206.55.132,0/24
Stati Uniti West-2/PDX	206.55.131,0/24
AP-Nord-Est-1/NRT	206.55.130.0/24
Stati Uniti Est-1/IAD	206.55129,0/24
AP-Sudest-2/SYD	206.55128,0/24

- Seleziona Rileva automaticamente l'IP esterno.
- Seleziona Richiedi TLS per le connessioni dai gateway di posta elettronica sopra elencati.
- Seleziona Salva nella parte inferiore della finestra di dialogo per salvare la configurazione. Una volta salvato, la console dell'amministratore mostrerà che il gateway in entrata è abilitato.

Configurazione di Microsoft Office 365 per l'inoltro SMTP in entrata (non autenticato)

L'esempio seguente mostra come configurare Microsoft Office 365 per l'utilizzo di un relay SMTP in entrata (non autenticato) di Mail Manager.

Prerequisiti

- Accesso all'interfaccia di amministrazione di Microsoft Security (Centro di amministrazione di Microsoft Security > Email e collaborazione > Criteri e regole > Criteri sulle minacce).
- Accesso al nameserver di dominio che ospita i record MX per i domini che verranno utilizzati per la configurazione di Mail Manager.

Per configurare Microsoft Office 365 per l'utilizzo di un relè SMTP in entrata

1. Aggiungere gli indirizzi IP di Mail Manager all'elenco Consenti
   a. Nell'interfaccia di amministrazione di Microsoft Security, vai a Email e collaborazione > Criteri e regole > Criteri sulle minacce.
   b. Seleziona Anti-spam in Norme.
   c. Seleziona Politica di filtro di connessione seguita da Modifica politica di filtro di connessione.
      - Nella finestra di dialogo Consenti sempre i messaggi dai seguenti indirizzi IP o intervallo di indirizzi, aggiungi gli IP degli endpoint di ingresso specifici per la tua regione dalla seguente tabella:

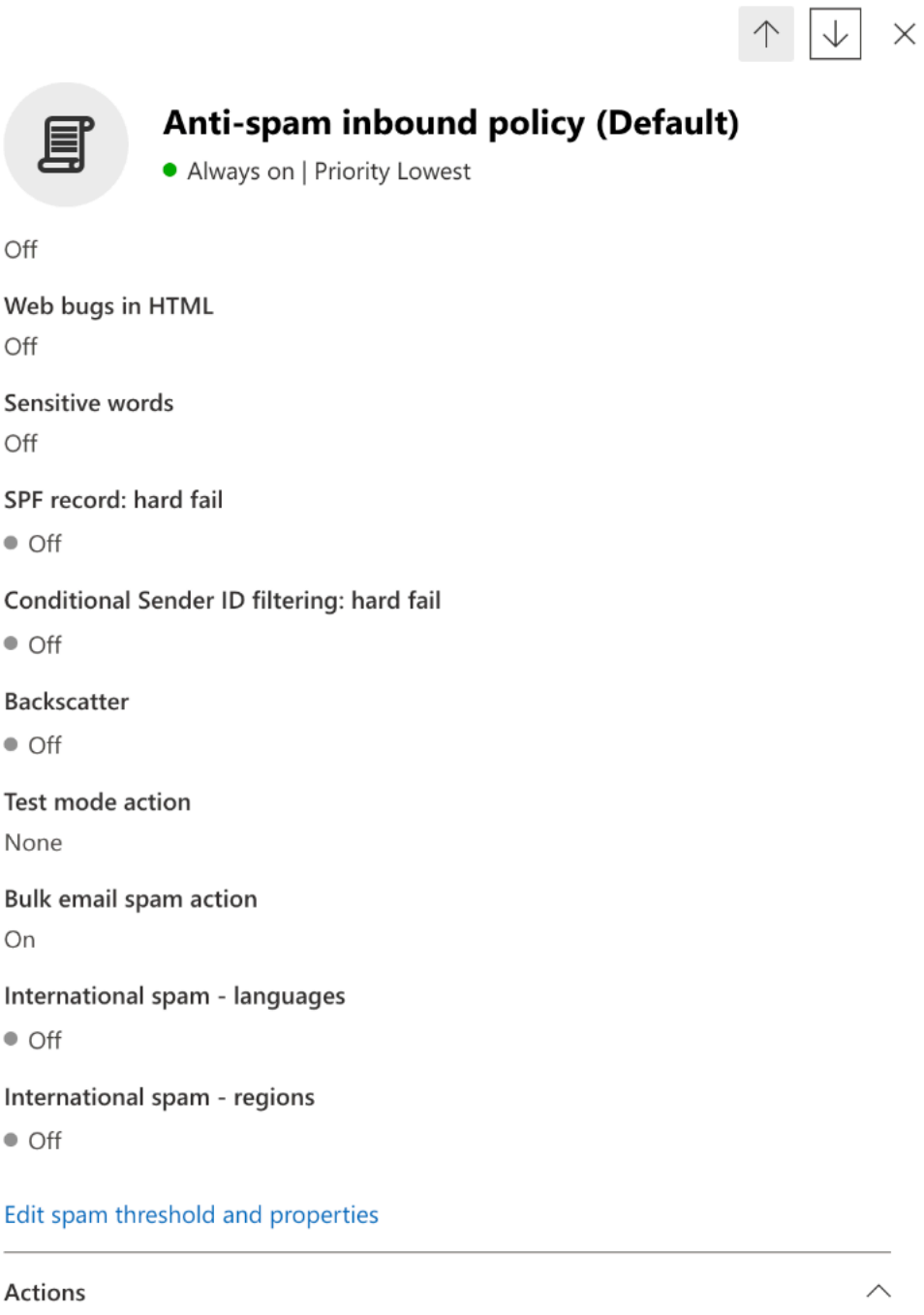
Regione	Intervallo IP
UE-West-1/DUB	206.55.133,0/24

Regione	Intervallo IP
UE-centrale-1/FRA	206.55.132,0/24
Stati Uniti West-2/PDX	206.55.131,0/24
AP-Nord-Est-1/NRT	206.55.130.0/24
Stati Uniti Est-1/IAD	206.55129,0/24
AP-Sudest-2/SYD	206.55128,0/24

- Seleziona Salva.

d. Torna all'opzione Anti-spam e scegli Politica anti-spam in entrata.

- Nella parte inferiore della finestra di dialogo, seleziona Modifica soglia e proprietà di spam:



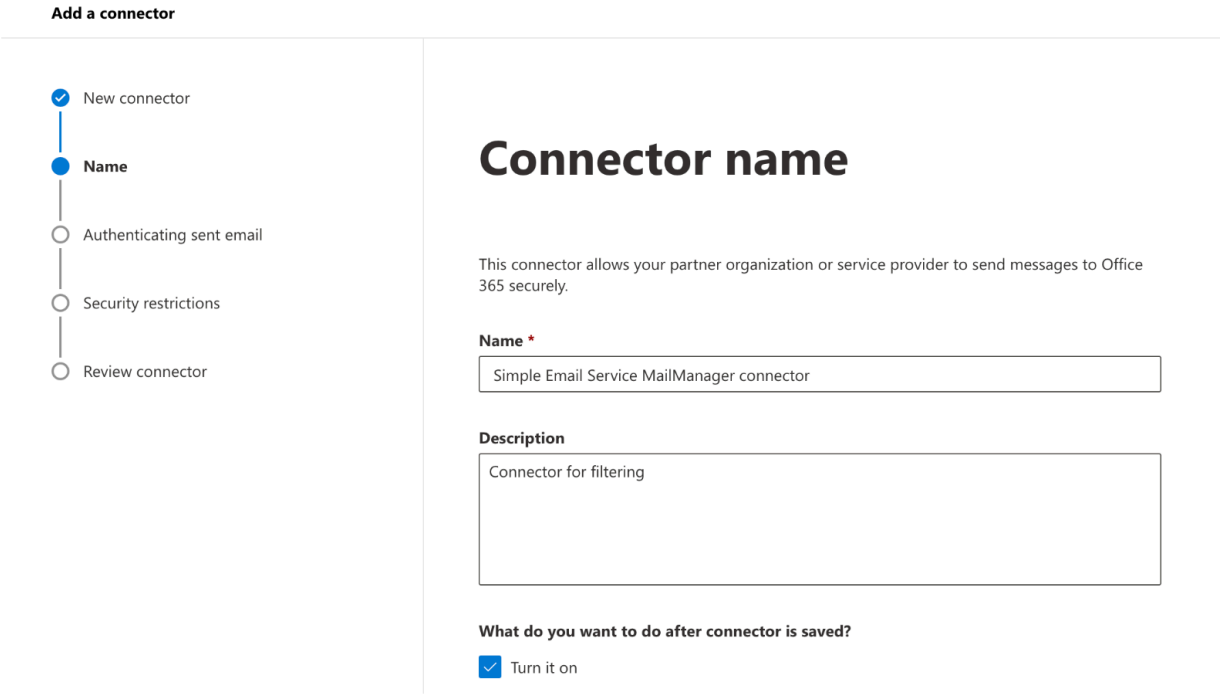
- Scorri fino a Contrassegna come spam e assicurati che il record SPF: hard fail sia impostato su Off.
- Seleziona Salva.

2. Configurazione di filtraggio avanzata (consigliata)

   Questa opzione consentirà a Microsoft Office 365 di identificare correttamente l'IP di connessione originale prima che il messaggio fosse ricevuto da SES Mail Manager.

a. Crea un connettore in entrata

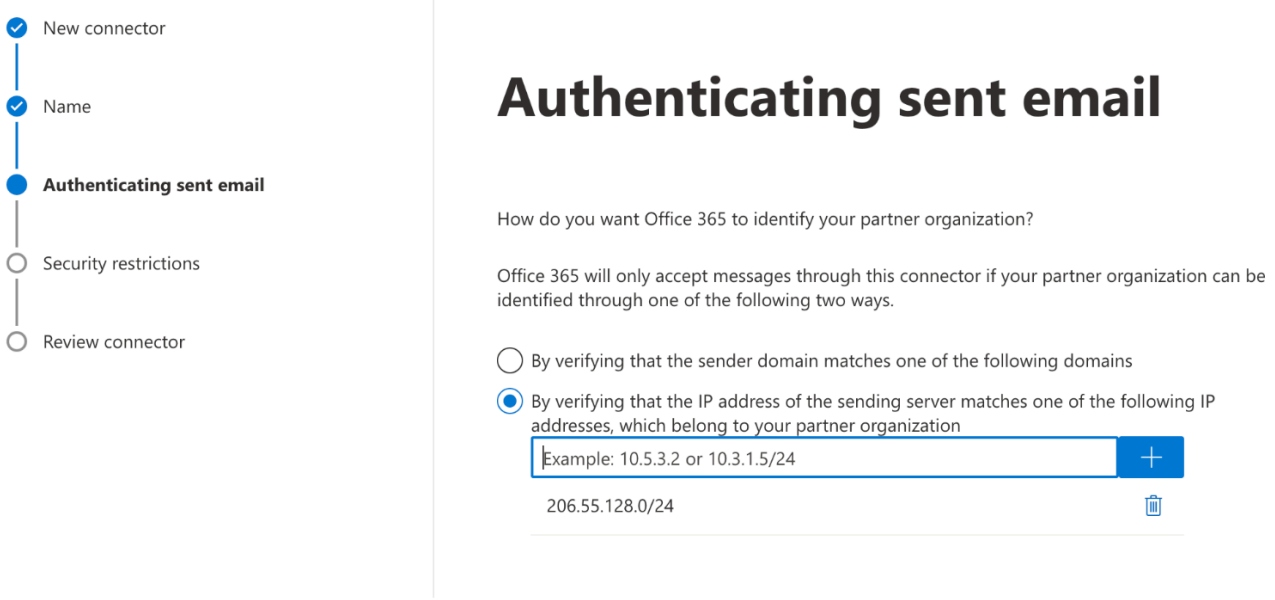
- Accedi alla nuova interfaccia di amministrazione di Exchange e vai a Mail flow > Connettori.
- Seleziona Aggiungi un connettore.
- In Connessione da, seleziona Organizzazione partner seguita da Avanti.
- Compila i campi come segue:
  - Nome: connettore Simple Email Service Mail Manager
  - Descrizione: connettore per il filtraggio



- Seleziona Avanti.
- In Autenticazione delle e-mail inviate, seleziona Verificando che l'indirizzo IP del server di invio corrisponda a uno dei seguenti indirizzi IP, che appartengono all'organizzazione partner, e aggiungi gli IP degli endpoint di ingresso specifici della tua regione dalla tabella seguente:

Regione	Intervallo IP
UE-West-1/DUB	206.55.133,0/24

Regione	Intervallo IP
UE-centrale-1/FRA	206.55.132,0/24
Stati Uniti West-2/PDX	206.55.131,0/24
AP-Nord-Est-1/NRT	206.55.130.0/24
Stati Uniti Est-1/IAD	206.55129,0/24
AP-Sudest-2/SYD	206.55128,0/24



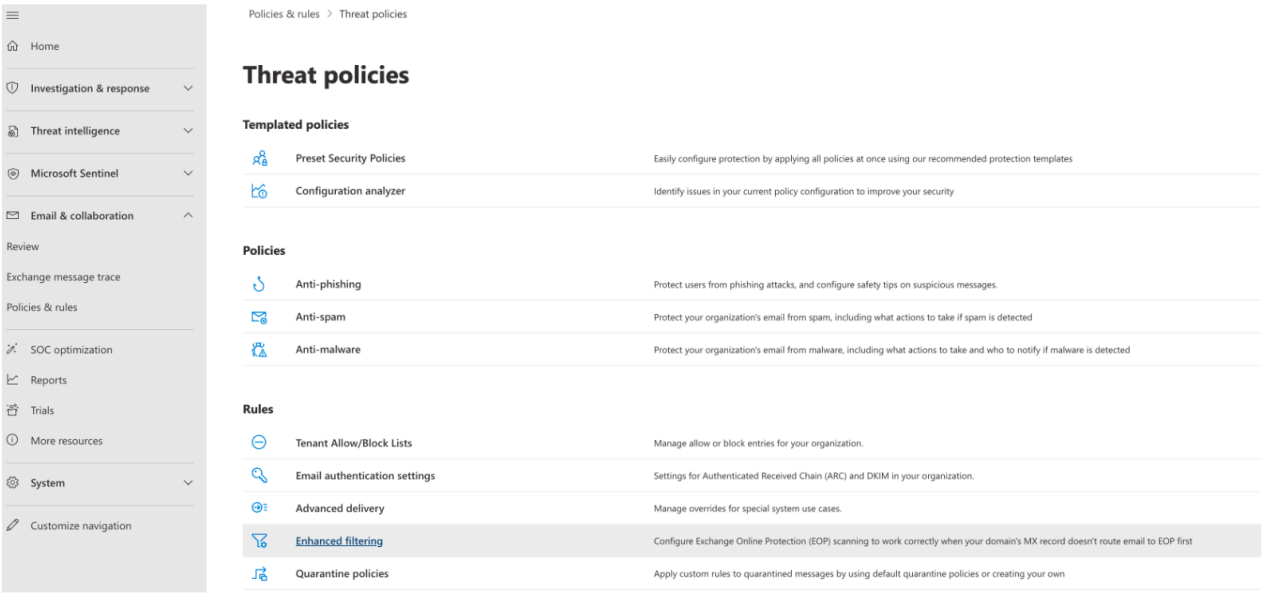
- Seleziona Avanti.
- In Restrizioni di sicurezza, accetta l'impostazione predefinita Rifiuta i messaggi di posta elettronica se non vengono inviati tramite TLS, seguita da Avanti.
- Controlla le impostazioni e seleziona Crea connettore.

b. Abilita il filtraggio avanzato

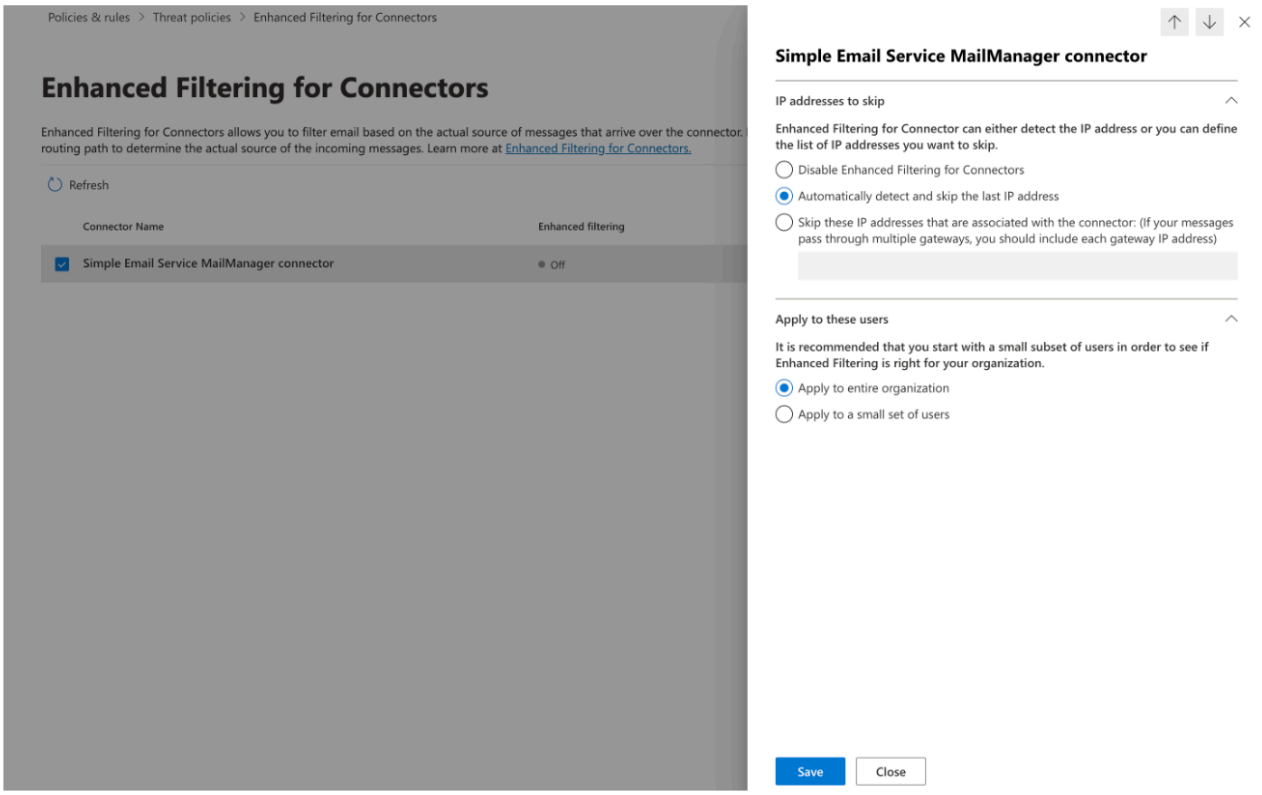
Ora che il connettore in ingresso è stato configurato, sarà necessario abilitare la configurazione di filtraggio avanzata del connettore nell'interfaccia di amministrazione di Microsoft Security.

- Nell'interfaccia di amministrazione di Microsoft Security, vai a Email e collaborazione > Criteri e regole > Criteri sulle minacce.

- Seleziona Filtro avanzato in Regole.



- Seleziona il connettore Simple Email Service Mail Manager che hai creato in precedenza per modificarne i parametri di configurazione.
- Seleziona Rileva automaticamente e ignora l'ultimo indirizzo IP e Applica all'intera organizzazione.



- Seleziona Salva.

Archiviazione delle e-mail

L'archiviazione delle e-mail consente di archiviare i tipi di e-mail specificati in arrivo nell'endpoint di ingresso, oltre a fornire un modo per trovare i messaggi archiviati attraverso un ricco set di filtri di ricerca avanzati e la possibilità di esportare i risultati.

L'archiviazione delle e-mail salva e protegge le e-mail archiviando i dati in uno spazio di archiviazione persistente e sicuro a lungo termine e offre un modo per cercare e archiviare rapidamente le e-mail. Fornisce un'archiviazione a tempo pieno a livello aziendale senza aumentare i requisiti di archiviazione del server di posta.

Quando l'endpoint di ingresso riceve e-mail, utilizza una politica di traffico per determinare quali e-mail bloccare o consentire. L'e-mail che autorizzi passa a un set di regole che applica regole condizionali per eseguire le azioni che hai definito per tipi specifici di e-mail. Una delle azioni della regola che puoi definire è l'azione di archiviazione: se selezioni questa azione, l'e-mail verrà archiviata nell'archivio e-mail designato.

È necessario innanzitutto creare un archivio prima di poterlo designare in un'azione della regola. La procedura riportata nella sezione successiva illustrerà come creare un archivio nella console SES.

Utilizzo dell'archiviazione delle e-mail nella console Amazon SES

La pagina di archiviazione delle e-mail nella console SES è composta da quattro tabelle interattive, Archivio di ricerca, Cronologia delle ricerche, Cronologia delle esportazioni e Gestione degli archivi, che puoi utilizzare per cercare e-mail negli archivi, esportare i risultati e gestire gli archivi. Nelle seguenti procedure, vengono fornite istruzioni per ogni tabella.

Per utilizzare la pagina di archiviazione delle e-mail per cercare, esportare e gestire gli archivi

1. Accedi AWS Management Console e apri la console Amazon SES all'indirizzo https://console.aws.amazon.com/ses/.
2. Nel pannello di navigazione a sinistra, scegli Archiviazione e-mail in Mail Manager.
3. La pagina di archiviazione delle e-mail è composta da quattro tabelle Archivio di ricerca, Cronologia delle ricerche, Cronologia delle esportazioni e Gestione degli archivi. Per istruzioni specifiche per ciascuna di queste tabelle, seleziona la scheda corrispondente di seguito:

Search archive

L'archivio di ricerca è una tabella interattiva che consente di cercare e trovare i messaggi archiviati con un ricco filtro e un set di date che offrono criteri di ricerca dettagliati per trovare qualsiasi messaggio, da un'e-mail specifica a molte e-mail che corrispondono a una categoria più ampia. I messaggi che corrispondono ai criteri di ricerca possono essere scaricati singolarmente o esportati in blocco in un bucket S3.

Per cercare, scaricare o esportare email archiviate

1. Nella pagina Archiviazione e-mail, scegli la scheda Cerca nell'archivio per visualizzare la tabella Cerca nell'archivio.
2. Fai clic all'interno del campo Archivio e scegli un archivio dall'elenco seguito da Cerca, oppure affina la ricerca utilizzando i seguenti passaggi.
3. Seleziona il campo Intervallo di date per espandere le opzioni di intervallo di date per la tua ricerca:

   - Intervallo relativo (predefinito): seleziona il pulsante di opzione corrispondente al numero di giorni desiderato oppure scegli un intervallo personalizzato selezionando un'unità di tempo e un intervallo di date fino a 30 giorni.
   - Intervallo assoluto: inserisci una data di inizio e una data di fine (e, se lo desideri, un'ora) fino a 30 giorni.

> **Note**
>
> - La ricerca all'interno di un archivio è limitata a 30 giorni alla volta. Ad esempio, se desideri cercare messaggi dal 1° giugno al 31 luglio, devi suddividerli in tre ricerche come segue:
>
>   1. 30 giorni a giugno.
>   2. I primi 30 giorni di luglio.
>   3. Il 31 luglio.
>
> - Per le date con intervallo relativo, l'ultimo giorno termina a mezzanotte. Ad esempio, se scegli Last 7 days (Ultimi 7 giorni), il settimo giorno sarà ieri, con termine a mezzanotte.

4. (Facoltativo) Seleziona il campo Filtri tra cui scegliere tra i seguenti filtri: From, To, CC, Subject line e Ha allegati. Si applicano le seguenti proprietà:

   - Puoi creare fino a 10 filtri.
   - Un filtro può essere modificato facendo clic su di esso o rimosso selezionando la X.

5. Scegli Cerca e l'e-mail archiviata che corrisponde ai criteri di ricerca verrà inserita nella tabella dei risultati della ricerca.

   - La colonna ID messaggio è nascosta per impostazione predefinita, ma può essere visualizzata selezionando l'icona a forma di ingranaggio per personalizzare la visualizzazione della tabella.
   - Ogni ricerca eseguita viene salvata automaticamente con un ID di ricerca univoco e verrà elencata nella tabella della cronologia delle ricerche.

6. Per visualizzare il testo di un messaggio insieme alle informazioni sulla busta e sull'intestazione, seleziona il pulsante di opzione del messaggio seguito da Visualizza dettagli per aprire la barra laterale dei dettagli del messaggio.
7. Per creare un file locale del messaggio, seleziona il pulsante di opzione del messaggio seguito da Scarica messaggio.
8. La ricerca filtrata può essere salvata in un bucket Amazon S3 selezionando Esporta in S3.

   a. Se conosci l'URI del bucket S3 che desideri utilizzare, inseriscilo nel campo URI S3; in caso contrario, scegli Sfoglia S3 e seleziona un bucket S3 e una cartella da utilizzare nella pagina S3.

   b. (Facoltativo) È possibile crittografare i messaggi esportati inserendo la propria AWS KMS chiave nel campo ARN della chiave KMS o selezionando Crea nuova chiave. Altrimenti, la crittografia verrà impostata sul metodo utilizzato nel bucket S3 di destinazione (anche se nessuno).

   c. Scegli Esporta e tutti i messaggi trovati nella ricerca filtrata verranno salvati come singoli file nella cartella S3 selezionata.

> **Note**
>
> Sebbene non ci siano limiti al numero di messaggi che l'archivio può contenere, i risultati della ricerca sono limitati a 1000 righe nella tabella dei risultati della ricerca.

Search history

In questa tabella è elencata una cronologia delle ricerche in modo da poter ripristinare il set di risultati o accedere a set di filtri complessi creati in precedenza. Puoi anche creare nuove ricerche basate sulla ricerca originale modificando i filtri e le date. Tutte le nuove ricerche vengono salvate automaticamente con un ID di ricerca univoco e verranno elencate in questa tabella.

Per visualizzare e utilizzare le ricerche precedenti

1. Nella pagina Archiviazione e-mail, scegli la scheda Cronologia delle ricerche per visualizzare la tabella Cronologia delle ricerche che elenca una cronologia di tutte le ricerche e-mail archiviate, con le più recenti in primo piano. Questa tabella carica i dati la prima volta che la visiti: se cambi scheda e torni indietro, usa l'icona di aggiornamento per recuperare i dati più recenti.
2. Fai clic all'interno del campo Archivio e scegli un archivio dall'elenco: tutte le ricerche appartenenti a quell'archivio verranno inserite nella tabella. Puoi visualizzare e fare di più con le ricerche individuali nei passaggi seguenti.
3. Seleziona il pulsante di opzione di una ricerca precedente seguito da Visualizza i risultati della ricerca per ripristinare i risultati di ricerca originali: si aprirà la pagina dell'archivio di ricerca che mostra il set di filtri e l'intervallo di date utilizzati per la ricerca originale insieme a tutti i messaggi trovati in precedenza in base a tali criteri. È possibile espandere la ricerca originale nei seguenti modi:
   - Crea una nuova ricerca modificando l'intervallo di date e i filtri seguiti da Cerca.
   - Tutte le nuove ricerche eseguite vengono salvate automaticamente con un ID di ricerca univoco e verranno elencate nella tabella della cronologia delle ricerche.

Export history

In questa tabella è elencata una cronologia delle esportazioni che consente un facile accesso al contenuto della cartella di esportazione nella console S3.

Per visualizzare le esportazioni recenti

1. Nella pagina Archiviazione e-mail, scegli la scheda Cronologia delle esportazioni per visualizzare la tabella Cronologia delle esportazioni che elenca tutte le ricerche e-mail archiviate che hai esportato in un bucket S3 negli ultimi 30 giorni. Questa tabella carica i dati

la prima volta che la visiti: se cambi scheda e torni indietro, usa l'icona di aggiornamento per recuperare i dati più recenti.

2. Se lo stato di un'esportazione è In coda, Preelaborazione o Elaborazione, puoi annullarla scegliendo Annulla.
3. Seleziona un URI S3 per aprire la cartella bucket dell'esportazione nella console S3, dove puoi vedere i file che contiene.

Manage archives

Questa tabella elenca gli archivi in cui sono disponibili le opzioni per creare un nuovo archivio, cercare un archivio particolare e visualizzarne i dettagli, modificare un archivio o eliminare un archivio.

Per creare e gestire archivi

1. Nella pagina Archiviazione e-mail, scegli la scheda Gestisci archivi per visualizzare la tabella Archivi che elenca tutti gli archivi di posta elettronica. Questa tabella carica i dati la prima volta che la visiti: se cambi scheda e torni indietro, usa l'icona di aggiornamento per recuperare i dati più recenti.
2. Per cercare un archivio particolare, inizia a digitare nel campo Archivi.
3. Per visualizzare i dettagli di un archivio, selezionane il nome nella colonna Nome archivio.
4. Per creare un archivio, seleziona Crea archivio.

    a. Inserisci un nome univoco nel campo Nome archivio.

    b. (Facoltativo) Seleziona un periodo di conservazione nel campo Periodo di conservazione per sostituire il periodo di conservazione predefinito di 180 giorni.

    c. (Facoltativo) È possibile crittografare l'archivio inserendo la propria AWS KMS chiave nel campo ARN della chiave KMS o selezionando Crea nuova chiave.

    Scegli Crea archivio.

5. Per modificare un archivio, seleziona il relativo pulsante di opzione seguito da Modifica.

    a. Modifica o cambia il nome nel campo Nome archivio.

    b. Modifica il periodo di conservazione nel campo Periodo di conservazione.

Scegli Aggiorna archivio.

6. Per eliminare un archivio, seleziona il relativo pulsante di opzione seguito da Elimina.

   - Digita `delete` nel campo Conferma seguito da Elimina.

     Lo stato dell'archivio passerà a In attesa di eliminazione nella tabella Archivi e verrà eliminato automaticamente dopo 30 giorni.

> **Note**
>
> Se desideri annullare questa eliminazione, crea un ticket per Amazon SES entro 30 giorni.

Componenti aggiuntivi via e-mail

Email Add-Ons è una raccolta di strumenti di sicurezza specializzati forniti da provider approvati da SES che possono essere utilizzati per gestire il tipo di e-mail consentite all'ingresso dell'endpoint di ingresso e per determinare le azioni da intraprendere su determinati tipi di e-mail. Questi strumenti sono soluzioni certificate per l'intelligence e l'applicazione della sicurezza, pronte per essere integrate nel flusso di lavoro di posta elettronica e attivabili direttamente dalla console di Mail Manager.

Questi componenti aggiuntivi offrono la flessibilità di scegliere tra soluzioni di sicurezza della posta elettronica verificate e adatte ai singoli casi d'uso, che possono essere utilizzate a un prezzo misurato, anziché acquistare una soluzione di prodotto singola di grandi dimensioni che potrebbe non essere ottimizzata per nessuna delle vostre esigenze. Email Add-Ons estende le sue principali funzionalità di intelligence sulle minacce e applicazione della sicurezza in base al carico di lavoro, quindi non c'è bisogno di indovinare la capacità richiesta. Questi vantaggi consentono di concentrarsi sull'anticipazione dei problemi di sicurezza delle e-mail e sul mantenimento di standard di servizio elevati per l'organizzazione.

Puoi saperne di più su ogni componente aggiuntivo direttamente dalla pagina Componenti aggiuntivi via e-mail nella console di Mail Manager, dove avrai accesso alle descrizioni dei prodotti, ai vantaggi principali e alle informazioni sui prezzi. Una volta deciso quale componente aggiuntivo utilizzare, è sufficiente abbonarsi ad esso dalla console di Mail Manager. Una volta effettuata l'iscrizione, potrai selezionarla come condizione della politica del traffico per determinare le e-mail

consentite a un dispositivo di ingresso o come condizione di set di regole per determinare le azioni da intraprendere su e-mail specifiche. Il supporto principale per tutti i componenti aggiuntivi è fornito AWS e accessibile anche dalla console di Mail Manager.

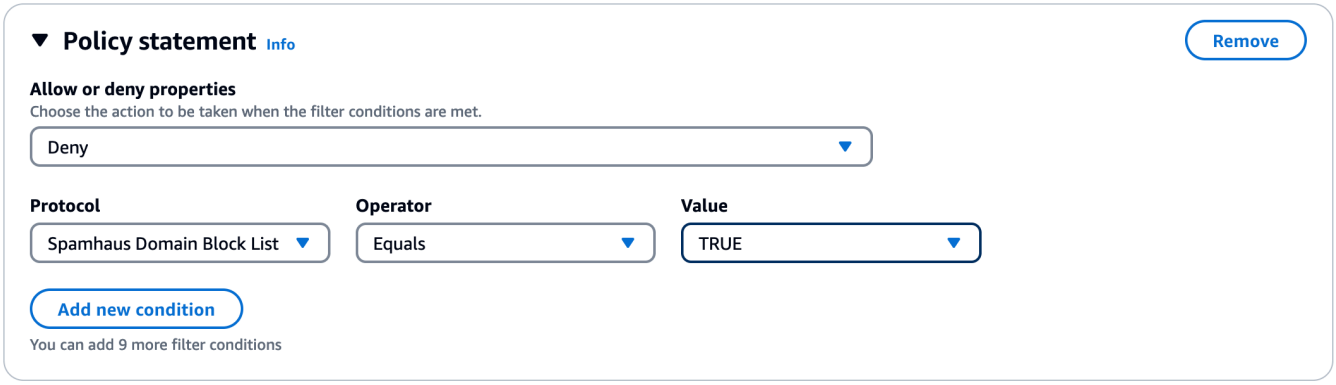
La procedura riportata nella sezione successiva ti illustrerà come iscriverti a un componente aggiuntivo di posta elettronica nella console di Mail Manager.

Iscrizione a Email Add-Ons nella console di Mail Manager

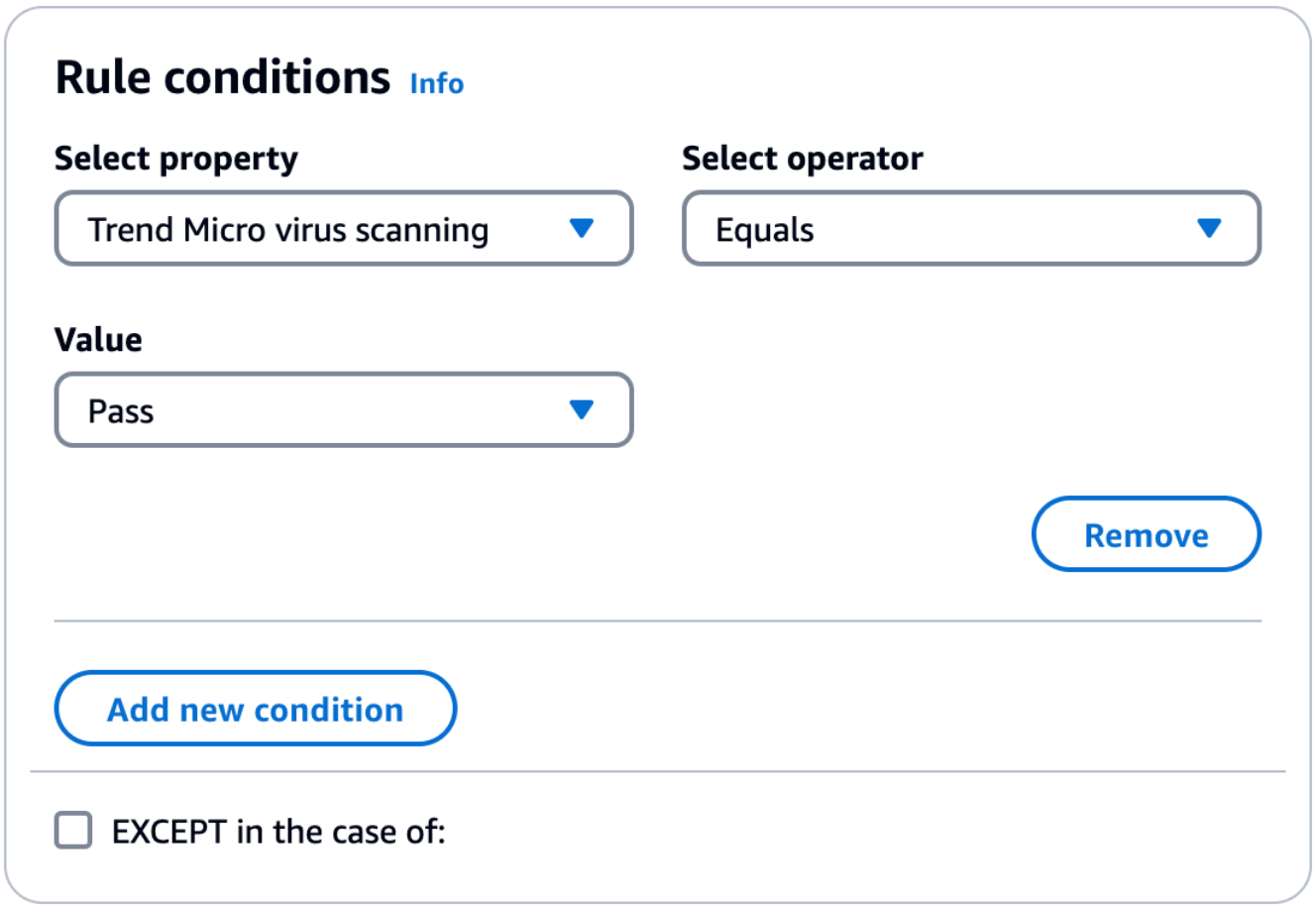
La procedura seguente mostra come utilizzare la pagina Componenti aggiuntivi di posta elettronica nella console di Mail Manager per sottoscrivere un componente aggiuntivo in modo che possa essere utilizzato in qualsiasi politica di traffico o set di regole.

Per iscriversi a un componente aggiuntivo e-mail utilizzando la console

1. Accedi AWS Management Console e apri la console Amazon SES all'indirizzo https://console.aws.amazon.com/ses/.
2. Nel pannello di navigazione a sinistra, scegli Email Add-Ons in Mail Manager.
3. Nella pagina Email Add-Ons, seleziona il titolo di qualsiasi scheda Add-On per aprire la relativa pagina di panoramica, dove puoi saperne di più sulle sue funzioni, sui vantaggi principali e sulle informazioni sui prezzi. Se desideri utilizzare questo componente aggiuntivo, scegli Iscriviti.
   - Leggi i Termini e condizioni presentati e seleziona la casella Accetto seguita da Iscriviti.
4. Dopo esserti abbonato a un componente aggiuntivo, potrai integrarlo nel tuo flusso di lavoro relativo alla posta elettronica selezionandolo come condizione della politica del traffico per negare o consentire l'accesso alla posta elettronica nel tuo endpoint di ingresso o come condizione del set di regole per determinare un'azione da intraprendere sui messaggi idonei. Gli esempi seguenti illustrano l'utilizzo di un componente aggiuntivo in una condizione di dichiarazione di policy e in una condizione di regola:
   - Utilizzo del componente aggiuntivo Spamhaus Domain Block List in una condizione di policy per bloccare la ricezione di email provenienti da un dominio elencato in Spamhaus e provenienti da un dominio elencato in Spamhaus:



- Per i dettagli su come creare politiche sul traffico e creare condizioni di dichiarazione delle politiche con Email Add-Ons, consulta. the section called “Creazione di politiche e dichiarazioni politiche sul traffico (console)”
- Utilizzo del componente aggiuntivo Trend Micro Virus Scanning in una condizione di regola per determinare un'azione della regola per le e-mail che superino la scansione antivirus:



- Per i dettagli su come creare set di regole e creare condizioni per le regole con Email Add-Ons, consultathe section called “Creazione di set di regole e regole (console)”.

5. Per visualizzare dettagli generali o accedere all'assistenza per qualsiasi componente aggiuntivo a cui sei abbonato, selezionane il nome nella pagina Componenti aggiuntivi via e-mail per aprirne la pagina di panoramica:

   - Nei dettagli generali puoi visualizzare la data di sottoscrizione e l'Amazon Resource Name (ARN) del tuo componente aggiuntivo.
   - Seleziona la scheda Support per accedere ai link a AWS Support.

6. Per annullare l'iscrizione a un componente aggiuntivo:

   a. Devi prima rimuoverlo da tutte le tue politiche sul traffico o dai set di regole in cui lo hai definito in una condizione; in caso contrario, i seguenti passaggi di annullamento dell'iscrizione non riusciranno.

   b. Seleziona il suo nome nella pagina Email Add-Ons per aprire la relativa pagina di panoramica seguita da Annulla l'iscrizione.

   c. Digita `confirm` nel campo Conferma seguito da Annulla iscrizione.

Politiche di autorizzazione per Mail Manager

Le politiche di questo capitolo sono fornite come unico punto di riferimento per le politiche necessarie per utilizzare tutte le diverse funzionalità di Mail Manager.

Nelle pagine delle funzionalità di Mail Manager, vengono forniti collegamenti che rimandano alla rispettiva sezione di questa pagina che contiene le politiche necessarie per utilizzare la funzionalità. Seleziona l'icona di copia della politica che ti serve e incollala come indicato nella descrizione della rispettiva funzionalità.

Le seguenti politiche consentono di utilizzare le diverse funzionalità contenute in Amazon SES Mail Manager tramite politiche e AWS Secrets Manager politiche di autorizzazione delle risorse. Se non conosci le politiche di autorizzazione, consulta the section called “Anatomia delle policy” e Politiche di autorizzazione per AWS Secrets Manager.

Politiche di autorizzazione per l'endpoint Ingress

Entrambe le policy di questa sezione sono necessarie per creare un endpoint di ingresso. Per informazioni su come creare un endpoint di ingresso e su dove utilizzare queste politiche, consulta. the section called “Creazione di un endpoint di ingresso (console)”

Secrets Manager: politica di autorizzazione delle risorse segrete per l'endpoint di ingresso

La seguente politica di autorizzazione delle risorse segrete di Secrets Manager è necessaria per consentire a SES di accedere al segreto utilizzando la risorsa ingress endpoint.

```
{
    "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/*"
                }
            }
        }
    ]
}
```

Politica relativa alle chiavi gestite dai clienti (CMK) di KMS per l'endpoint di ingresso

La seguente politica relativa alle chiavi gestite dai clienti (CMK) di KMS è necessaria per consentire a SES di utilizzare la chiave mentre utilizza la chiave segreta.

```
{
    "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/*"
        }
    }
}
```

Politiche di autorizzazione per l'inoltro SMTP

Entrambe le policy di questa sezione sono necessarie per creare un relè SMTP. Per informazioni su come creare un relè SMTP e dove utilizzare queste politiche, consulta. the section called “Creazione di un relè SMTP (console)”

Secrets Manager: politica di autorizzazione delle risorse segrete per l'inoltro SMTP

La seguente politica di autorizzazione delle risorse segrete di Secrets Manager è necessaria per consentire a SES di accedere al segreto utilizzando la risorsa di inoltro 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/*"
                }
            }
        }
    ]
}
```

Politica delle chiavi CMK (Customer Managed Key) di KMS per il relè SMTP

La seguente politica di chiave CMK (Customer Managed Key) di KMS è necessaria per consentire a SES di utilizzare la chiave mentre utilizza la chiave segreta.

```
{
    "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/*"
                }
            }
        }
    ]
}
```

Politiche di autorizzazione per l'archiviazione delle e-mail

Criteri di identità IAM di archiviazione di base

Queste sono le policy di identità IAM per l'autorizzazione delle operazioni di archiviazione. Queste politiche da sole potrebbero non essere sufficienti per alcune operazioni (vedi Archiviazione della crittografia a riposo con KMS CMK e Archiving export).

```
{
    "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"
            ]
        }
    ]
}
```

Archiviazione ed esportazione

Queste sono le policy di identità IAM (oltre alle policy di archiviazione di base di cui sopra) necessarie. `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/*"
        }
    ]
}
```

Questa è la politica per il bucket di destinazione.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "ses.amazonaws.com"
            },
            "Action": [
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
            "Resource": "arn:aws:s3:::MyDestinationBucketName"
        },
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "ses.amazonaws.com"
            },
            "Action": [
                "s3:PutObject",
                "s3:PutObjectAcl",
                "s3:PutObjectTagging",
                "s3:GetObject"
            ],
            "Resource": "arn:aws:s3:::MyDestinationBucketName/*"
        }
    ]
}
```

> **Note**
>
> L'archiviazione non supporta chiavi sostitutive confuse (aws:SourceArn, aws:SourceAccount, aws: SourceOrg ID o aws:SourceOrgPaths). Questo perché l'archiviazione delle e-mail di Mail Manager previene il problema del confuso vice verificando se l'identità chiamante dispone delle autorizzazioni di scrittura per il bucket di destinazione dell'esportazione utilizzando Forward Access Sessions prima di iniziare l'esportazione effettiva.

Archiviazione della crittografia inattiva con KMS CMK

Si tratta della crittografia inutilizzata con le policy KMS Customer Managed Keys (CMK) (oltre alle politiche di archiviazione di base di cui sopra) necessarie per creare e utilizzare gli archivi (richiamando qualsiasi API di archiviazione).

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Action": [
            "kms:DescribeKey",
            "kms:Decrypt",
            "kms:GenerateDataKey"
        ],
        "Resource": "arn:aws:kms:us-west-2:111122223333:key/MyKmsKeyArnID"
    }
}
```

Questa è la politica chiave KMS richiesta per l'archiviazione delle e-mail.

```
{
    "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": "*"
        }
    ]
}
```

Politiche di autorizzazione e fiducia per l'esecuzione delle azioni relative alle regole

Il ruolo di esecuzione delle regole SES è un ruolo AWS Identity and Access Management (IAM) che concede l'autorizzazione all'esecuzione delle regole per accedere a AWS servizi e risorse. Prima di creare una regola in un set di regole, è necessario creare un ruolo IAM con una policy che consenta l'accesso alle AWS risorse richieste. SES assume questo ruolo durante l'esecuzione di un'azione relativa a una regola. Ad esempio, potresti creare un ruolo di esecuzione delle regole con l'autorizzazione a scrivere un messaggio di posta elettronica in un bucket S3 come azione di regola da intraprendere quando le condizioni della regola sono soddisfatte.

Pertanto, oltre ai criteri di autorizzazione individuali di questa sezione, necessari per eseguire le azioni delle regole Write to S3, Delivery to mailbox e Invia a Internet, sono necessari i seguenti criteri di attendibilità.

```
{
    "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/
*"
          }
        }
      }
    ]
  }
```

Politica di autorizzazione per l'azione della regola Write to S3

La seguente politica è necessaria per utilizzare l'azione della regola Write to S3 che recapita l'e-mail ricevuta a un bucket S3.

```
{
    "Version": "2012-10-17",
    "Statement": [
      {
        "Effect": "Allow",
        "Action": "s3:PutObject",
        "Resource": "arn:aws:s3:::MyDestinationBucketName/*"
      }
    ]
  }
```

Politica di autorizzazione per l'azione relativa alla regola Deliver to mailbox

La seguente politica è necessaria per utilizzare l'azione della regola Delivery to mailbox che recapita l'e-mail ricevuta a un WorkMail account Amazon.

```
{
    "Version": "2012-10-17",
    "Statement": [
      {
        "Effect": "Allow",
        "Action": ["workmail:DeliverToMailbox"],
        "Resource": "arn:aws:workmail:us-
east-1:888888888888:organization/MyWorkMailOrganizationID>"
      }
    ]
  }
```

Politica di autorizzazione per l'azione relativa alla regola Invia a Internet

La seguente politica è necessaria per utilizzare l'azione della regola Invia a Internet che invia l'e-mail ricevuta a un dominio esterno.

```
{
    "Version": "2012-10-17",
    "Statement": [
      {
        "Effect": "Allow",
        "Action": ["ses:SendEmail", "ses:SendRawEmail"],
        "Resource": "arn:aws:ses:us-east-1:888888888888:identity/example.com"
      }
    ]
  }
```

Gestione di elenchi e sottoscrizioni in Amazon Simple Email Service

Puoi gestire i tuoi elenchi per l'invio di e-mail e le sottoscrizioni, nonché per l'eliminazione delle e-mail in Amazon SES. Per aiutarti a preservare la reputazione del mittente, Amazon SES offre elenchi di eliminazione a livello di account e a livello di set di configurazione che impediscono l'invio a destinatari non validi e la compromissione della tua reputazione di mittente. Come ulteriore misura contro il mancato recapito di e-mail e i reclami, SES può aggiungere automaticamente collegamenti di annullamento dell'iscrizione a tutta la posta in uscita tramite la gestione delle sottoscrizioni.

Ognuno di questi tipi di elenchi è discusso in dettaglio nelle sezioni elencate negli argomenti di questo capitolo; tuttavia, viene presentata una panoramica degli elenchi di eliminazione, perché esistono tre tipi di elenchi di eliminazione e una modifica chiave con gestione globale degli elenchi di eliminazione. Si suggerisce di leggere questa panoramica prima di lavorare con uno degli elenchi discussi in questo capitolo.

Panoramica dei tre tipi di elenchi di eliminazione

La caratteristica di rimozione dell'elenco di eliminazione globale non è più rivolta al cliente e non interagisci più con essa per gestire gli elenchi di eliminazione. L'elenco globale di eliminazione opera ed è gestito in background da SES. In qualità di cliente, ora hai a disposizione elenchi di eliminazione a livello di account ed elenchi di eliminazione a livello di set di configurazione che ti offrono un controllo più personalizzato di come gestisci l'eliminazione delle e-mail per il tuo account.

Di seguito vengono illustrati i diversi tipi di elenchi di eliminazione, il loro ambito e i vantaggi che offrono. I tre tipi di elenchi di eliminazione utilizzati in Amazon SES sono:

- Elenco di eliminazione globale: di proprietà e gestito da SES per proteggere la reputazione degli indirizzi nel pool di IP condiviso SES.
- Elenco di eliminazione a livello di account: di proprietà e gestito dal cliente per proteggere la reputazione del suo account, sostituisce l'elenco di eliminazione globale.
- Eliminazione a livello di set di configurazione: di proprietà e gestito dal cliente per fornire un controllo condizionale o granulare della gestione degli elenchi di eliminazione, - sovrascrive l'elenco di eliminazione a livello di account.

L'elenco di eliminazione globale era l'unico tipo di elenco di eliminazione fino all'introduzione dell'eliminazione a livello di account e a livello di set di configurazione nella nuova console Amazon

SES e nell'API v2. L'elenco di eliminazione globale è di proprietà e gestito da SES per proteggere la reputazione di SES. Questo è necessario perché tutti i clienti SES condividono lo stesso pool di indirizzi IP (a meno che non dispongano di IP dedicati), perciò è importante che SES assicuri che i clienti non inviino spam o qualsiasi altro tipo di messaggio che influisca negativamente sulla reputazione di tali indirizzi IP nel pool di IP condiviso SES. Sebbene non si interagisca più direttamente con l'elenco di eliminazione globale, esso funziona ancora in background e i principi generali relativi al funzionamento di tale elenco possono essere applicati anche per illustrare i principi generali relativi al funzionamento degli altri tipi di elenchi di eliminazione. Per informazioni, consultare Elenco di eliminazione globale Amazon SES.

> **Note**
>
> Il modulo di richiesta di rimozione dell'elenco di eliminazione globale non è presente nella console Amazon SES, perché l'elenco di eliminazione a livello di account lo ha sostituito per tutti i vantaggi spiegati in questa sezione.

L'elenco di eliminazione a livello di account è stato introdotto in modo che i clienti possano creare e controllare i propri elenchi di eliminazione e la reputazione, pertanto l'elenco di eliminazione a livello di account si applica solo al tuo account. L'interfaccia dell'elenco di eliminazione a livello di account nella nuova console fornisce un modo semplice per gestire gli indirizzi nell'elenco di eliminazione a livello di account, incluse le operazioni in blocco per aggiungere o rimuovere indirizzi. Se un indirizzo è incluso nell'elenco di eliminazione globale, ma non nel tuo elenco di eliminazione a livello di account (il che significa che vuoi eseguire un invio ad esso) e invii ad esso, Amazon SES tenterà comunque la consegna, ma in caso di mancato recapito, quest'ultimo influirà sulla tua reputazione, ma nessun altro otterrà mancati recapiti perché non può eseguire un invio a quell'indirizzo e-mail se non utilizza il proprio elenco di eliminazione a livello di account. Pertanto, l'elenco di eliminazione a livello di account sovrascrive l'elenco di eliminazione globale solo per il tuo account. Per informazioni, consultare Utilizzo dell'elenco di eliminazione a livello di account di Amazon SES.

L'eliminazione a livello di set di configurazione ti consente di configurare le personalizzazioni di eliminazione e le sovrascritture nell'eliminazione a livello di account tramite l'uso di più set di configurazione creati appositamente per diversi scenari di invio di e-mail. Ad esempio, se l'elenco di eliminazione a livello di account è configurato sia per l'aggiunta di indirizzi di mancato recapito che di reclamo, ma hai definito un determinato demographic di e-mail in un set di configurazione per il quale sei interessato solo all'aggiunta di indirizzi di reclamo, puoi farlo abilitando questa eliminazione del set di configurazione in modo che gli indirizzi e-mail vengano aggiunti all'elenco di eliminazione a livello di account solo per i reclami (non mancati recapiti e reclami come è impostato nell'elenco di

eliminazione a livello di account) dall'e-mail inviata con questo set di configurazione. Con l'elenco di eliminazione a livello di set di configurazione, esistono diversi livelli di sovrascrittura dell'eliminazione a livello di account, incluso il non utilizzo dell'eliminazione. Per informazioni, consultare Utilizzo dell'eliminazione a livello di set di configurazione per ignorare l'elenco di eliminazione a livello di account.

Elenco di eliminazione globale Amazon SES

Amazon SES mantiene un elenco di eliminazione globale interno che opera ed è gestito in background da SES. Quando un cliente SES invia un messaggio e-mail che genera in un mancato recapito permanente, SES aggiunge l'indirizzo e-mail che ha prodotto il mancato recapito a un elenco di eliminazione globale. L'elenco di eliminazione è globale nel senso che si applica a tutti i clienti SES. In altre parole, se un cliente diverso tenta di inviare un messaggio e-mail a un indirizzo presente nell'elenco di eliminazione globale, SES accetta il messaggio, ma non lo invia, perché l'indirizzo e-mail è eliminato.

La funzionalità di richiesta di rimozione dell'indirizzo e-mail dell'elenco di eliminazione globale non è più rivolta al cliente e non interagisci più con essa per gestire gli elenchi di eliminazione. Per sostituire questa funzionalità, ora Amazon SES offre un nuovo modo per gestire gli elenchi di eliminazione rendendo disponibili elenchi di eliminazione a livello di account ed elenchi di eliminazione a livello di set di configurazione che offrono un controllo maggiormente personalizzato relativo alla gestione dell'eliminazione delle e-mail per il tuo account. Per ulteriori informazioni, consulta Utilizzo dell'elenco di eliminazione a livello di account di Amazon SES e Utilizzo dell'eliminazione a livello di set di configurazione per ignorare l'elenco di eliminazione a livello di account.

> **Important**
>
> Il modulo di richiesta di rimozione degli indirizzi e-mail dell'elenco di eliminazione globale non è presente nella console Amazon SES perché l'elenco di eliminazione a livello di account lo ha sostituito. Per informazioni su come utilizzare l'elenco di eliminazione a livello di account, consulta Utilizzo dell'elenco di eliminazione a livello di account di Amazon SES.

Considerazioni sull'elenco di eliminazione globale

Fattori chiave relativi all'elenco di eliminazione globale:

- L'elenco globale di eliminazione opera ed è gestito in background da SES: non è possibile interagirci direttamente; tuttavia, puoi sovrascriverlo utilizzando l'elenco di eliminazione a livello di account.
- L'elenco di eliminazione globale è abilitato per impostazione predefinita per tutti gli account SES. Non puoi disabilitarlo.
- Poiché SES applica l'elenco di eliminazione globale a tutti i clienti, non è possibile eseguire query sull'elenco di eliminazione globale o aggiungervi indirizzi manualmente.
- Quando un indirizzo e-mail produce un mancato recapito permanente, SES aggiunge l'indirizzo all'elenco di eliminazione globale per un breve periodo di tempo. Trascorso tale periodo di tempo, SES rimuove l'indirizzo dall'elenco. Se l'indirizzo produce un altro mancato recapito permanente, SES lo aggiunge nuovamente all'elenco di eliminazione globale per un periodo di tempo maggiore e lo rimuove al termine di tale periodo. Il periodo di tempo in cui un indirizzo rimane nell'elenco di eliminazione globale aumenta ogni volta che l'indirizzo produce un mancato recapito permanente. Un indirizzo e-mail può rimanere nell'elenco di eliminazione globale per un periodo massimo di 14 giorni.
- Se tenti di inviare un messaggio a un indirizzo nell'elenco di eliminazione globale, SES accetta il messaggio ma non lo invia. SES genera una notifica di mancato recapito con un valore `bounceType` di `Permanent` e un valore `bounceSubType` di `Suppressed`. Ricevere questo tipo di notifica di mancato recapito è l'unico modo per sapere se un indirizzo è incluso nell'elenco di eliminazione globale. Non puoi eseguire query sull'elenco di eliminazione globale.
- SES conteggia i messaggi che invii agli indirizzi dell'elenco di eliminazione globale rispetto alla percentuale di mancati recapiti del tuo account e alla tua quota di invio giornaliera.
- Come per qualsiasi indirizzo e-mail che abbia generato un mancato recapito permanente, devi rimuovere gli indirizzi per i quali un elenco di eliminazione determini un mancato recapito dalla tua mailing list, a meno che tu non abbia certezza circa la validità dell'indirizzo.
- I mancati recapiti dell'elenco di eliminazione sono considerati per il calcolo della percentuale di mancati recapiti dell'account. Se la frequenza di mancato recapito è troppo elevata, il tuo account potrebbe venire incluso in una fase di verifica o la sua capacità di inviare e-mail potrebbe venire sospesa.

> **Note**
>
> È importante capire come i tre elenchi di eliminazione SES sono correlati e la loro gerarchia. Consulta Panoramica dei tre tipi di elenchi di eliminazione.

Utilizzo dell'elenco di eliminazione a livello di account di Amazon SES

L'elenco di eliminazione a livello di account di Amazon SES è stato introdotto in modo che i clienti possano creare e controllare i propri elenchi di eliminazione e la reputazione, pertanto il tuo elenco di eliminazione a livello di account si applica solo al tuo account. L'interfaccia dell'elenco di eliminazione a livello di account nella console SES fornisce un modo semplice per gestire gli indirizzi nell'elenco di eliminazione a livello di account, incluse operazioni per aggiungere o rimuovere indirizzi in blocco.

L'elenco di eliminazione a livello di account di SES si applica solo al tuo Account AWS nella Regione AWS corrente. Puoi aggiungere o rimuovere, singolarmente o in blocco, indirizzi dall'elenco di eliminazione a livello di account utilizzando l'API SES v2 o la console.

> **Note**
>
> Per aggiungere o rimuovere in blocco gli indirizzi, è necessario disporre dell'accesso di produzione. Per ulteriori informazioni sulla sandbox, consulta Richiedi l'accesso alla produzione (uscita dalla sandbox di Amazon SES).

Considerazioni sull'elenco di eliminazione a livello di account di Amazon SES

Quando si utilizza l'elenco di eliminazione a livello di account, è necessario considerare i seguenti fattori:

- Se hai iniziato a utilizzare Amazon SES dopo il 25 novembre 2019, l'account utilizza l'elenco di eliminazione a livello di account per impostazione predefinita sia per i mancati recapiti che per i reclami. Se hai iniziato a utilizzare SES prima di questa data, è necessario abilitare questa funzionalità tramite l'operazione `PutAccountSuppressionAttributes` nell'API SES.
- Se tenti di inviare un messaggio a un indirizzo che si trova nell'elenco di eliminazione a livello di account con un motivo per l'eliminazione che corrisponde allo stesso motivo scelto per le impostazioni dell'eliminazione a livello di account , SES accetta il messaggio, ma non lo invia; tuttavia, se n on corrispondono, allora SES lo invia. Per chiarire questo punto, vengono forniti i seguenti esempi:

  - Hai impostato l'eliminazione a livello di account con il motivo di eliminazione di solo Bounce e SES non tenterà di recapitare gli indirizzi presenti nell'elenco di eliminazione a livello di account il cui motivo di eliminazione è Bounce.
  - Hai impostato l'eliminazione a livello di account con il motivo di eliminazione di Bounce e lamentele e SES non tenterà di recapitare gli indirizzi presenti nell'elenco di eliminazione a livello di account il cui motivo di eliminazione è Bounce o Lamentela.
  - Hai impostato l'eliminazione a livello di account con il motivo di eliminazione di solo Bounce e SES tenterà di recapitare gli indirizzi presenti nell'elenco di eliminazione a livello di account il cui motivo di eliminazione è Lamentela (poiché, in questo caso, non coincidono).
- SES non conteggia i messaggi inviati agli indirizzi presenti nell'elenco di eliminazione a livello di account ai fini della frequenza di mancato recapito o di reclami del tuo account.
- Se un indirizzo si trova nell'elenco di eliminazione globale, ma non in quello a livello di account (il che significa che vuoi spedire a tale indirizzo) e viene inviata un'email a tale indirizzo, SES proverà a inviarla; tuttavia, se torna indietro, viene comunque conteggiata ai fini della frequenza di mancato recapito del tuo account e della quota di invio giornaliera.
- SES conteggia i messaggi inviati agli indirizzi presenti nell'elenco di eliminazione a livello di account ai fini della quota di invio giornaliera.
- Gli indirizzi e-mail nell'elenco di eliminazione a livello di account rimangono al suo interno fino a quando non li rimuovi.
- Se la capacità del tuo account di inviare e-mail viene sospesa, dopo 90 giorni SES elimina automaticamente gli indirizzi presenti nell'elenco di eliminazione a livello di account. Se la capacità del tuo account di inviare e-mail viene ripristinata prima del termine di questo periodo di 90 giorni, gli indirizzi nell'elenco non vengono eliminati.
- Gmail non fornisce dati di reclamo a SES. Se un destinatario utilizza il pulsante Spam nel client Web Gmail per segnalare un messaggio ricevuto come spam, non viene aggiunto all'elenco di eliminazione a livello di account.
- Puoi abilitare l'elenco di eliminazione a livello di account se l'account si trova nella sandbox SES. Tuttavia, non puoi utilizzare il comando PutSuppressedDestination o CreateImportJob fino a quando l'account non viene rimosso dalla sandbox. Per ulteriori informazioni sulla sandbox, consulta Richiedi l'accesso alla produzione (uscita dalla sandbox di Amazon SES).
- Solo i mancati recapiti permanenti vengono aggiunti all'elenco di eliminazione a livello di account. Per ulteriori informazioni sulla differenza tra un'e-mail non recapitata e un mancato recapito permanente, consulta the section called "Dopo l'invio di un e-mail da parte di Amazon SES".

- Quando utilizzi l'elenco di eliminazione a livello di account, SES aggiunge all'elenco di eliminazione globale anche gli indirizzi che provocano mancati recapiti permanenti.

Abilitazione dell'elenco di eliminazione a livello di account di Amazon SES

È possibile utilizzare il comando PutAccountSuppressionAttributes nell'API Amazon SES v2 per abilitare e configurare l'elenco di eliminazione a livello di account. Puoi configurare rapidamente e facilmente questa impostazione utilizzando l'AWS CLI. Per ulteriori informazioni sull'installazione e la configurazione dell'AWS CLI, consulta la Guida per l'utente di AWS Command Line Interface.

Configurazione dell'elenco di eliminazione a livello di account tramite la AWS CLI

- Nella riga di comando, inserisci il comando seguente:

  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
  ```

  Per abilitare l'elenco di eliminazione a livello di account, è necessario specificare almeno un motivo per il parametro `suppressed-reasons`. È possibile specificare `BOUNCE` o `COMPLAINT` oppure entrambi, come mostrato nell'esempio precedente.

Per configurare l'elenco di eliminazione a livello di account tramite la console SES:

1. Accedi alla AWS Management Console e apri la console Amazon SES all'indirizzo https://console.aws.amazon.com/ses/.
2. Nel pannello di navigazione, in Configuration (Configurazione) scegli Suppression list (Elenco di eliminazione).
3. Nel riquadro Account-level settings (Impostazioni a livello di account), scegliEdit (Modifica).
4. In Suppression list (Elenco di eliminazione), seleziona la casella Enabled (Abilitato).

5. In Suppression reasons (Motivi eliminazione), seleziona uno dei motivi per cui gli indirizzi e-mail del destinatario devono essere aggiunti automaticamente all'elenco di eliminazione a livello di account.
6. Seleziona Salva modifiche.

Abilitazione dell'elenco di eliminazione a livello di account di Amazon SES per un set di configurazione

Puoi anche configurare l'eliminazione a livello di account di Amazon SES in modo che si applichi solo a specifici set di configurazione. In questo caso, gli indirizzi vengono aggiunti all'elenco di eliminazione solo se hai specificato il set di configurazione quando hai inviato l'e-mail che ha causato l'evento di mancato recapito o reclamo.

> **Note**
>
> La procedura seguente presuppone che sia già installata l'AWS CLI. Per ulteriori informazioni sull'installazione e la configurazione dell'AWS CLI, consulta la Guida per l'utente di AWS Command Line Interface.

Configurazione dell'elenco di eliminazione a livello di account per un set di configurazione utilizzando la AWS CLI

- Nella riga di comando, inserisci il comando seguente:

  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
  ```

Nell'esempio precedente, sostituire *configSet* con il nome del set di configurazione che deve utilizzare l'elenco di eliminazione a livello di account.

Per configurare l'elenco di eliminazione a livello di account per un set di configurazione tramite la console SES:

1. Accedi alla AWS Management Console e apri la console Amazon SES all'indirizzo https://console.aws.amazon.com/ses/.
2. Nel pannello di navigazione, in Configuration (Configurazione), scegli Configuration sets (Set di configurazione).
3. In Configuration sets (Set di configurazione), scegli il nome del set di configurazione che vuoi configurare con l'eliminazione personalizzata.
4. Nel riquadro Suppression list options (Opzioni elenco di eliminazione), scegli Edit (Modifica).
5. La sezione Suppression list options (Opzioni elenco di eliminazione) fornisce un set di decisioni per definire l'eliminazione personalizzata a partire dall'opzione di utilizzare questo set di configurazione per sovrascrivere l'eliminazione a livello di account. La mappa logica di eliminazione a livello di set di configurazione ti aiuterà a comprendere gli effetti delle combinazioni di sovrascrittura. Queste selezioni su più livelli di sovrascrittura possono essere combinate per implementare tre diversi livelli di eliminazione:

   a. Use account-level suppression (Usa eliminazione a livello di account): non sovrascrivere l'eliminazione a livello di account e non implementare alcuna eliminazione a livello di set di configurazione. Fondamentalmente, qualsiasi e-mail inviata utilizzando questo set di configurazione utilizzerà solo l'eliminazione a livello di account. Per farlo:

      - In Suppression list settings (Impostazioni elenco di eliminazione), deseleziona la casella Override account level settings (Sovrascrivi impostazioni a livello di account).

   b. Do not use any suppression (Non usare alcuna eliminazione): sovrascrivi l'eliminazione a livello di account senza abilitare l'eliminazione a livello di set di configurazione. Questo significa che qualsiasi e-mail inviata utilizzando questo set di configurazione non utilizzerà alcuna eliminazione a livello di account. In altre parole, tutta l'eliminazione viene annullata. Per farlo:

i. In Suppression list settings (Impostazioni elenco di eliminazione), controlla la casella Override account level settings (Sovrascrivi impostazioni a livello di account).

ii. In Suppression list (Elenco di eliminazione), deseleziona la casella Enabled (Abilitato).

c. Use configuration set-level suppression (Usa eliminazione a livello di set di configurazione): sostituisci l'eliminazione a livello di account con impostazioni personalizzate dell'elenco di eliminazione definite in questo set di configurazione. Questo significa che qualsiasi e-mail inviata utilizzando questo set di configurazione utilizzerà solo le proprie impostazioni di eliminazione e ignorerà le impostazioni di eliminazione a livello di account. Per farlo:

i. In Suppression list settings (Impostazioni elenco di eliminazione), controlla la casella Override account level settings (Sovrascrivi impostazioni a livello di account).

ii. In Suppression list (Elenco di eliminazione), seleziona Enabled (Abilitato).

iii. In Specify the reason(s)… (Specificare i motivi…), seleziona uno dei motivi dell'eliminazione da utilizzare per questo set di configurazione.

6. Seleziona Salva modifiche.

Aggiunta di singoli indirizzi e-mail all'elenco di eliminazione a livello di account di Amazon SES

È possibile aggiungere singoli indirizzi all'elenco di eliminazione a livello di account tramite l'operazione PutSuppressedDestination nell'API SES v2. Non è previsto alcun limite al numero di indirizzi che è possibile aggiungere all'elenco di eliminazione a livello di account.

> **Note**
>
> La procedura seguente presuppone che sia già installata l'AWS CLI. Per ulteriori informazioni sull'installazione e la configurazione dell'AWS CLI, consulta la Guida per l'utente di AWS Command Line Interface.

Aggiunta di singoli indirizzi all'elenco di eliminazione a livello di account tramite la AWS CLI

- Nella riga di comando, inserisci il comando seguente:

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
```

Nell'esempio precedente, sostituire *recipient@example.com* con l'indirizzo e-mail che si desidera aggiungere all'elenco di eliminazione a livello di account e *BOUNCE* con il motivo per cui si sta aggiungendo l'indirizzo all'elenco di eliminazione (i valori accettabili sono `BOUNCE` e `COMPLAINT`).

Aggiunta di singoli indirizzi all'elenco di eliminazione a livello di account tramite la console SES:

1. Accedi alla AWS Management Console e apri la console Amazon SES all'indirizzo https://console.aws.amazon.com/ses/.
2. Nel pannello di navigazione, in Configuration (Configurazione) scegli Suppression list (Elenco di eliminazione).
3. Nel riquadro Suppression list (Elenco di eliminazione), scegli Add email address (Aggiungi indirizzo e-mail).
4. Inserisci un indirizzo e-mail in Email address (Indirizzo e-mail) e seleziona un motivo in Suppression reason (Motivo eliminazione). Per aggiungere altri indirizzi, scegli Enter another address (Aggiungi un altro indirizzo) e ripeti l'operazione per ogni indirizzo aggiuntivo.
5. Al termine dell'inserimento degli indirizzi, controlla che tutte le voci siano corrette. Se decidi che una delle voci non dovrebbe far parte di questo invio, seleziona il rispettivo pulsante Remove (Rimuovi).
6. Scegli Save changes (Salva modifiche) per aggiungere gli indirizzi e-mail inseriti all'elenco di eliminazione a livello di account.

Aggiunta di indirizzi e-mail in blocco all'elenco di eliminazione a livello di account di Amazon SES

Puoi aggiungere gli indirizzi in blocco caricando il tuo elenco di contatti in un oggetto Amazon S3 ed eseguendo poi l'operazione CreateImportJob nell'API Amazon SES v2.

> **Note**
>
> - Non è previsto alcun limite al numero di indirizzi che è possibile aggiungere all'elenco di eliminazione a livello di account, ma è previsto un limite di aggiunta in blocco di 100.000 indirizzi in un oggetto Simple Storage Service (Amazon S3) per ogni chiamata API.
> - Se l'origine dati è un bucket S3, deve esistere nella stessa regione in cui viene importato.

Per aggiungere indirizzi e-mail in blocco all'elenco di eliminazione a livello di account, completare la seguente procedura.

- Carica il tuo elenco di indirizzi in un oggetto Amazon S3 in formato CSV o JSON.

  Esempio di formato CSV per l'aggiunta di indirizzi:

  recipient1@example.com,*BOUNCE*

  recipient2@example.com,*COMPLAINT*

  Sono supportati solo i file JSON delimitati da nuova riga. In questo formato, ogni riga è un oggetto JSON completo che contiene una singola definizione di indirizzo.

  Esempio di formato JSON per l'aggiunta di indirizzi:

  {"emailAddress":"*recipient1@example.com*","reason":"*BOUNCE*"}

  {"emailAddress":"*recipient2@example.com*","reason":"*COMPLAINT*"}

  Nell'esempio precedente sostituire *recipient1@example.com* e *recipient2@example.com* con gli indirizzi e-mail che si desidera aggiungere all'elenco di eliminazione a livello di account. I motivi accettabili per cui aggiungere gli indirizzi all'elenco di soppressione sono *BOUNCE* e *COMPLAINT*.
- Concedi a SES l'autorizzazione a leggere l'oggetto Amazon S3.

Se applicata a un bucket Amazon S3, la seguente policy concede a SES l'autorizzazione a leggere tale bucket. Per maggiori informazioni sulle policy dei bucket per Amazon S3, consulta Utilizzo delle policy dei bucket e dell'utente nella Guida per l'utente di 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"
                }
            }
        }
    ]
}
```

- Concedi a SES l'autorizzazione a utilizzare la chiave AWS KMS.

  Se l'oggetto Amazon S3 è crittografato con una chiave AWS KMS, devi concedere ad Amazon SES l'autorizzazione a utilizzare la chiave AWS KMS. SES può ottenere l'autorizzazione solo da una chiave gestita dal cliente, non da una chiave KMS di default. Devi concedere a SES l'autorizzazione a utilizzare la chiave gestita dal cliente aggiungendo un'istruzione alla policy della chiave.

  Incolla la seguente istruzione nella policy della chiave per consentire a SES di utilizzare la tua chiave gestita dal cliente.

```
{
   "Sid": "AllowSESToDecrypt",
   "Effect": "Allow",
   "Principal": {
       "Service":"ses.amazonaws.com"
   },
```

```
    "Action": [
        "kms:Decrypt",
    ],
    "Resource": "*"
}
```

- Utilizzo del comando CreateImportJob nell'API SES v2.

> **Note**
>
> L'esempio seguente presuppone che sia già installata l'AWS CLI. Per ulteriori informazioni sull'installazione e la configurazione dell'AWS CLI, consulta la Guida per l'utente di AWS Command Line Interface.

Nella riga di comando, immetti il comando seguente: Sostituire *s3bucket* con il nome del bucket Amazon S3 ed *s3object* con il nome dell'oggetto Amazon S3.

```
aws sesv2 create-import-job --import-destination
 SuppressionListDestination={SuppressionListImportAction=PUT} --import-data-source
 S3Url=s3://s3bucket/s3object,DataFormat=CSV
```

Per aggiungere indirizzi e-mail in blocco all'elenco di eliminazione a livello di account tramite la console SES:

1. Accedi alla AWS Management Console e apri la console Amazon SES all'indirizzo https://console.aws.amazon.com/ses/.
2. Nel pannello di navigazione, in Configuration (Configurazione) scegli Suppression list (Elenco di eliminazione).
3. Nella tabella Suppression list (Elenco di eliminazione), espandi il pulsante Bulk actions (Operazioni in blocco) e seleziona Add email addresses in bulk (Aggiungi indirizzi e-mail in blocco).
4. In Bulk action specifications (Specifiche operazione in blocco), seleziona (a)Choose file from S3 bucket (Scegli file dal bucket S3) o (b)Import from file (Importa da file). Sono previste procedure per ciascun metodo di importazione:

    a. Choose file from S3 bucket (Scegli file dal bucket S3): se il file di origine è già archiviato in un bucket Amazon S3:

i. Se conosci l'URI del bucket Amazon S3 che vuoi utilizzare, inseriscilo nel campo Amazon S3 URI (URI Amazon S3); in caso contrario, scegli Browse S3 (Sfoglia S3):

A. In Buckets (Bucket), seleziona il nome del bucket S3.

B. In Objects (Oggetti), seleziona il nome del file, quindi seleziona Choose (Scegli): verrà riaperta la schermata Bulk action specifications (Specifiche operazione in blocco).

C. (Facoltativo) Se vuoi tornare alla console Amazon S3 per visualizzare i dettagli sul tuo oggetto S3, scegli View (Visualizza).

ii. In File format (Formato file), seleziona il formato del file che hai scelto di importare dal tuo bucket Amazon S3.

iii. Scegli Add email addresses (Aggiungi indirizzi e-mail) per avviare l'importazione di indirizzi dal tuo file: viene visualizzata una tabella sotto la scheda Bulk actions (Operazioni in blocco).

b. Import from file (Importa da file): se disponi di un file di origine locale da caricare su un bucket Amazon S3 nuovo o esistente:

i. In Import source file (Importa file di origine), seleziona Choose file (Scegli file).

ii. Seleziona il file JSON o CSV nel browser dei file e scegli Open (Apri): vedrai il nome, la dimensione e la data del tuo file sotto il pulsante Choose file (Scegli file).

iii. Espandi Amazon S3 bucket (Bucket Amazon S3) e seleziona il bucket S3.

- Per caricare il file in un nuovo bucket, scegli Create S3 bucket (Crea bucket S3), inserisci un nome nel campo Bucket name (Nome bucket) e scegli Create bucket (Crea bucket).

iv. Scegli Add email addresses (Aggiungi indirizzi e-mail) per avviare l'importazione di indirizzi dal tuo file: viene visualizzata una tabella nella scheda Bulk actions (Operazioni in blocco).

5. Indipendentemente dal metodo di importazione utilizzato, il tuo ID processo sarà elencato in Bulk actions (Operazioni in blocco) insieme al tipo di importazione, allo stato e alla data: per visualizzare i dettagli del processo, seleziona l'ID processo.

6. Seleziona la scheda Suppression list (Elenco di eliminazione) e tutti gli indirizzi e-mail importati correttamente verranno visualizzati con il relativo motivo dell'eliminazione e la data aggiunti; sono disponibili le seguenti opzioni:

a. Seleziona un indirizzo e-mail o seleziona la casella di controllo corrispondente e scegli View report (Visualizza report) per visualizzarne i dettagli. Se si tratta di un indirizzo aggiunto automaticamente al tuo elenco di eliminazione a causa di un mancato recapito o di un reclamo, verranno visualizzate informazioni sull'evento di feedback che ne ha causato l'aggiunta, inclusi i dettagli sul messaggio e-mail che ha prodotto l'evento di attivazione.

b. Seleziona la casella di controllo corrispondente di uno o più indirizzi e-mail che desideri rimuovere dall'elenco di eliminazione dell'account e scegli Remove (Rimuovi).

Visualizzazione di un elenco di indirizzi presenti nell'elenco di eliminazione a livello di account di Amazon SES

È possibile visualizzare un elenco di tutti gli indirizzi e-mail presenti nell'elenco di eliminazione a livello di account per l'account tramite il comando ListSuppressedDestinations nell'API SES v2.

> **Note**
>
> La procedura seguente presuppone che sia già installata l'AWS CLI. Per ulteriori informazioni sull'installazione e la configurazione dell'AWS CLI, consulta la Guida per l'utente di AWS Command Line Interface.

Visualizzazione di un elenco di tutti gli indirizzi e-mail presenti nell'elenco di eliminazione a livello di account

- Nella riga di comando, inserisci il comando seguente:

```
aws sesv2 list-suppressed-destinations
```

Il comando precedente restituisce tutti gli indirizzi e-mail presenti nell'elenco di eliminazione a livello di account per l'account in questione. L'output è simile a quello riportato di seguito.

```
{
    "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: se il tuo output include un campo "NextToken" con un valore della stringa, indica che ci sono ulteriori indirizzi e-mail nell'elenco di eliminazione per il tuo account. Per visualizzare questi ulteriori indirizzi eliminati, invia un'altra richiesta a `ListSuppressedDestinations` e passa il valore della stringa restituito nel parametro `--next-token` in questo modo:

  ```
  aws sesv2 list-suppressed-destinations --next-token string
  ```

  Nel comando precedente, sostituire *`stringa`* con il valore NextToken restituito.

  Per ulteriori informazioni, consulta How to list over 1000 email addresses from account-level suppression list.

È possibile utilizzare l'opzione `StartDate` per visualizzare solo gli indirizzi e-mail aggiunti all'elenco dopo una determinata data.

Visualizzazione di un elenco di indirizzi aggiunti all'elenco di eliminazione a livello di account dopo una data specifica

- Nella riga di comando, inserisci il comando seguente:

  ```
  aws sesv2 list-suppressed-destinations --start-date 1604394130
  ```

  Nel comando precedente, sostituire *`1604394130`* con il timestamp Unix della data di inizio.

È inoltre possibile utilizzare l'opzione `EndDate` per visualizzare solo gli indirizzi e-mail aggiunti all'elenco prima di una determinata data.

Visualizzazione di un elenco di indirizzi aggiunti all'elenco di eliminazione a livello di account prima di una data specifica

- Nella riga di comando, inserisci il comando seguente:

  ```
  aws sesv2 list-suppressed-destinations --end-date 1611126000
  ```

  Nel comando precedente, sostituire *1611126000* con il timestamp Unix della data di fine.

Nella riga di comando Linux, macOS o Unix, è anche possibile utilizzare l'utility `grep` integrata per cercare indirizzi o domini specifici.

Ricerca di un indirizzo specifico nell'elenco di eliminazione a livello di account

- Nella riga di comando, inserisci il comando seguente:

  ```
  aws sesv2 list-suppressed-destinations | grep -A2 'example.com'
  ```

  Nel comando precedente, sostituire *example.com* con la stringa di testo (ad esempio l'indirizzo o il dominio) che si desidera cercare.

Visualizzazione di un elenco di tutti gli indirizzi e-mail presenti nell'elenco di eliminazione a livello di account tramite la console SES:

1. Accedi alla AWS Management Console e apri la console Amazon SES all'indirizzo https://console.aws.amazon.com/ses/.
2. Nel pannello di navigazione, in Configuration (Configurazione) scegli Suppression list (Elenco di eliminazione).
3. Nel riquadro Suppression list (Elenco di eliminazione), tutti gli indirizzi e-mail nell'elenco di eliminazione a livello di account vengono visualizzati con il relativo motivo dell'eliminazione e la data aggiunti; sono disponibili le seguenti opzioni:

   a. Seleziona un indirizzo e-mail o seleziona la casella di controllo corrispondente e scegli View report (Visualizza report) per visualizzarne i dettagli. Se si tratta di un indirizzo aggiunto

automaticamente al tuo elenco di eliminazione a causa di un mancato recapito o di un reclamo, verranno visualizzate informazioni sull'evento di feedback che ne ha causato l'aggiunta, inclusi i dettagli sul messaggio e-mail che ha prodotto l'evento di attivazione.

b. Puoi personalizzare la tabella dell'elenco di eliminazione scegliendo l'icona a forma di ingranaggio: verrà visualizzata una finestra modale in cui puoi personalizzare le dimensioni della pagina, il ritorno a capo e le colonne da visualizzare. Dopo aver effettuato le selezioni, scegli Confirm (Conferma). La tabella dell'elenco di eliminazione rifletterà le tue scelte di visualizzazione.

Rimozione di singoli indirizzi e-mail dall'elenco di eliminazione a livello di account di Amazon SES

Se un indirizzo si trova nell'elenco di eliminazione del tuo account per errore, puoi rimuoverlo tramite l'operazione DeleteSuppressedDestination nell'API SES v2.

> **Note**
>
> La procedura seguente presuppone che sia già installata l'AWS CLI. Per ulteriori informazioni sull'installazione e la configurazione dell'AWS CLI, consulta la Guida per l'utente di AWS Command Line Interface.

Rimozione di singoli indirizzi dall'elenco di eliminazione a livello di account tramite la AWS CLI

- Nella riga di comando, inserisci il comando seguente:

  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
  ```

Nell'esempio precedente, sostituire *recipient@example.com* con l'indirizzo e-mail che si desidera rimuovere dall'elenco di eliminazione a livello di account.

Rimozione di singoli indirizzi dall'elenco di eliminazione a livello di account tramite la console SES:

1. Accedi alla AWS Management Console e apri la console Amazon SES all'indirizzo https://console.aws.amazon.com/ses/.
2. Nel pannello di navigazione, in Configuration (Configurazione) scegli Suppression list (Elenco di eliminazione).
3. Rimuovi i singoli indirizzi e-mail tramite (a) la selezione dalla tabella o (b) l'inserimento mediante digitazione:

    a. Selezione dalla tabella: nella tabella Suppression list (Elenco di eliminazione), seleziona la casella di controllo corrispondente a uno o più indirizzi e-mail e scegli Remove (Rimuovi).

    b. Inserimento mediante digitazione:

        i. Nella tabella Suppression list (Elenco di eliminazione), scegli Remove email address (Rimuovi indirizzo e-mail).

        ii. Inserisci un indirizzo e-mail in Email address. Per aggiungere altri indirizzi, scegli Enter another address (Inserisci un altro indirizzo) e ripeti l'operazione per ogni indirizzo aggiuntivo.

        iii. Al termine dell'inserimento degli indirizzi, controlla che tutte le voci siano corrette. Se decidi che una delle voci non dovrebbe far parte di questo invio, seleziona il rispettivo pulsante Remove (Rimuovi).

        iv. Scegli Save changes (Salva modifiche) per rimuovere gli indirizzi e-mail specificati dall'elenco di eliminazione a livello di account.

Rimozione di indirizzi e-mail in blocco dall'elenco di eliminazione a livello di account di Amazon SES

Puoi rimuovere gli indirizzi in blocco caricando il tuo elenco di contatti in un oggetto Amazon S3 ed eseguendo poi l'operazione CreateImportJob nell'API SES v2.

> **Note**
>
> - Non è previsto alcun limite al numero di indirizzi che è possibile rimuovere dall'elenco di eliminazione a livello di account, ma è previsto un limite di eliminazione in blocco di 10.000 indirizzi in un oggetto Amazon S3 per ogni chiamata API.
> - Se l'origine dati è un bucket S3, deve esistere nella stessa regione in cui viene importato.

Per rimuovere indirizzi e-mail in blocco dall'elenco di eliminazione a livello di account, completare la seguente procedura.

- Carica il tuo elenco di indirizzi in un oggetto Amazon S3 in formato CSV o JSON.

  Esempio di formato CSV per la rimozione degli indirizzi:

  recipient3@example.com

  Sono supportati solo i file JSON delimitati da nuova riga. In questo formato, ogni riga è un oggetto JSON completo che contiene una singola definizione di indirizzo.

  Esempio di formato JSON per l'aggiunta di indirizzi:

  `{"emailAddress":"`*recipient3@example.com*`"}`

  Nell'esempio precedente, sostituire *recipient3@example.com* con l'indirizzo e-mail che si desidera rimuovere dall'elenco di eliminazione a livello di account.
- Concedi a SES l'autorizzazione a leggere l'oggetto Amazon S3.

  Se applicata a un bucket Amazon S3, la seguente policy concede a SES l'autorizzazione a leggere tale bucket. Per maggiori informazioni sulle policy dei bucket per Amazon S3, consulta Utilizzo delle policy dei bucket e dell'utente nella Guida per l'utente di 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"
                }
            }
        }
    ]
}
```

- Concedi a SES l'autorizzazione a utilizzare la chiave AWS KMS.

  Se l'oggetto Amazon S3 è crittografato con una chiave AWS KMS, devi concedere ad Amazon SES l'autorizzazione a utilizzare la chiave AWS KMS. SES può ottenere l'autorizzazione solo da una chiave gestita dal cliente, non da una chiave KMS di default. Devi concedere a SES l'autorizzazione a utilizzare la chiave gestita dal cliente aggiungendo un'istruzione alla policy della chiave.

  Incolla la seguente istruzione nella policy della chiave per consentire a SES di utilizzare la tua chiave gestita dal cliente.

```
{
   "Sid": "AllowSESToDecrypt",
   "Effect": "Allow",
   "Principal": {
       "Service":"ses.amazonaws.com"
   },
   "Action": [
       "kms:Decrypt",
   ],
   "Resource": "*"
}
```

- Utilizzo del comando CreateImportJob nell'API SES v2.

> **Note**
>
> L'esempio seguente presuppone che sia già installata l'AWS CLI. Per ulteriori informazioni sull'installazione e la configurazione dell'AWS CLI, consulta la Guida per l'utente di AWS Command Line Interface.

Nella riga di comando, immetti il comando seguente: Sostituire *s3bucket* con il nome del bucket Amazon S3 e *s3object* con il nome dell'oggetto Amazon S3.

```
aws sesv2 create-import-job --import-destination
 SuppressionListDestination={SuppressionListImportAction=DELETE} --import-data-source
 S3Url="s3://s3bucket/s3object",DataFormat=CSV
```

Per rimuovere indirizzi e-mail in blocco dall'elenco di eliminazione a livello di account tramite la console SES:

1. Accedi alla AWS Management Console e apri la console Amazon SES all'indirizzo https://console.aws.amazon.com/ses/.
2. Nel pannello di navigazione, in Configuration (Configurazione) scegli Suppression list (Elenco di eliminazione).
3. Nella tabella Suppression list (Elenco di eliminazione), espandi il pulsante Bulk actions (Operazioni in blocco) e seleziona Remove email addresses in bulk (Rimuovi indirizzi e-mail in blocco).
4. In Bulk action specifications (Specifiche operazione in blocco), seleziona (a) Choose file from S3 bucket (Scegli file dal bucket S3) o (b) Import from file (Importa da file). Sono previste procedure diverse per ciascun metodo di importazione:

    a. Choose file from S3 bucket (Scegli file dal bucket S3): se il file di origine è già archiviato in un bucket Amazon S3:

        i. Se conosci l'URI del bucket Amazon S3 che vuoi utilizzare, inseriscilo nel campo Amazon S3 URI (URI Amazon S3); in caso contrario, scegli Browse S3 (Sfoglia S3):

            A. In Buckets (Bucket), seleziona il nome del bucket S3.

            B. In Objects (Oggetti), seleziona il nome del file, quindi seleziona Choose (Scegli): verrà riaperta la schermata Bulk action specifications (Specifiche operazione in blocco).

C. (Facoltativo) Se vuoi tornare alla console Amazon S3 per visualizzare i dettagli sul tuo oggetto S3, scegli View (Visualizza).

ii. In File format (Formato file), seleziona il formato del file che hai scelto di importare dal bucket Amazon S3.

iii. Scegli Remove email addresses (Rimuovi indirizzi e-mail) per avviare l'importazione di indirizzi dal tuo file: viene visualizzata una tabella nella scheda Bulk actions (Operazioni in blocco).

b. Import from file (Importa da file): se disponi di un file di origine locale da caricare su un bucket Amazon S3 nuovo o esistente:

i. In Import source file (Importa file di origine), seleziona Choose file (Scegli file).

ii. Seleziona il file JSON o CSV nel browser dei file e scegli Open (Apri): vedrai il nome, la dimensione e la data del tuo file sotto il pulsante Choose file (Scegli file).

iii. Espandi Amazon S3 bucket (Bucket Amazon S3) e seleziona il bucket S3.

- Per caricare il file in un nuovo bucket, scegli Create S3 bucket (Crea bucket S3), inserisci un nome nel campo Bucket name (Nome bucket) e scegli Create bucket (Crea bucket).

iv. Scegli Remove email addresses (Rimuovi indirizzi e-mail) per avviare l'importazione di indirizzi dal tuo file: viene visualizzata una tabella nella scheda Bulk actions (Operazioni in blocco).

5. Indipendentemente dal metodo di importazione utilizzato, il tuo ID processo sarà elencato in Bulk actions (Operazioni in blocco) insieme al tipo di importazione, allo stato e alla data: per visualizzare i dettagli del processo, seleziona l'ID processo.
6. Seleziona la scheda Suppression list (Elenco di eliminazione) e tutti gli indirizzi e-mail importati correttamente rimossi dall'elenco di eliminazione non verranno più visualizzati.

Visualizzazione di un elenco di processi di importazione per l'account

È possibile visualizzare un elenco di tutti gli indirizzi e-mail presenti nell'elenco di eliminazione a livello di account per l'account in questione utilizzando il comando ListImportJobs nell'API Amazon SES v2.

> **Note**
>
> La procedura seguente presuppone che sia già installata l'AWS CLI. Per ulteriori informazioni sull'installazione e la configurazione dell'AWS CLI, consulta la Guida per l'utente di AWS Command Line Interface.

Visualizzazione di un elenco di tutti i processi di importazione per l'account

- Nella riga di comando, inserisci il comando seguente:

```
aws sesv2 list-import-jobs
```

Il comando precedente restituisce tutti i processi di importazione per l'account. L'output è simile a quello riportato di seguito.

```
{
    "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"
        }
    ]
}
```

Per visualizzare un elenco di tutti i processi di importazione per l'account tramite la console SES:

1. Accedi alla AWS Management Console e apri la console Amazon SES all'indirizzo https://console.aws.amazon.com/ses/.
2. Nel pannello di navigazione, in Configuration (Configurazione) scegli Suppression list (Elenco di eliminazione).
3. Nel riquadro Suppression list (Elenco di eliminazione), seleziona la scheda Bulk actions (Operazioni in blocco).
4. Tutti i processi di importazione saranno elencati nella tabella Bulk actions (Operazioni in blocco) insieme al tipo di importazione, allo stato e alla data.
5. Per visualizzare i dettagli del processo, seleziona l'ID processo e verranno visualizzati i riquadri seguenti:

    a. Bulk action status (Stato operazione in blocco): mostra lo stato generale dei processi, l'ora e la data di completamento, il numero di record importati e il numero di record che non sono stati importati correttamente.

    b. Bulk action details (Dettagli operazione in blocco): mostra l'ID processo, indipendentemente dal fatto che sia stato utilizzato per aggiungere o rimuovere indirizzi, se il formato di file era JSON o CSV, l'URI del bucket Amazon S3 in cui è stato archiviato il file in blocco e l'ora e la data di creazione dell'operazione in blocco.

Recupero di informazioni di un processo di importazione per l'account

È possibile ottenere informazioni su un processo di importazione per l'account utilizzando il comando GetImportJob nell'API Amazon SES v2.

> **Note**
>
> La procedura seguente presuppone che sia già installata l'AWS CLI. Per ulteriori informazioni sull'installazione e la configurazione dell'AWS CLI, consulta la Guida per l'utente di AWS Command Line Interface.

Recupero di informazioni su un processo di importazione per l'account

- Nella riga di comando, inserisci il comando seguente:

```
aws sesv2 get-import-job --job-id JobId
```

Il comando precedente restituisce informazioni su un processo di importazione per l'account. L'output è simile a quello riportato di seguito.

```
{
    "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"
}
```

Per ottenere informazioni su un processo di importazione per l'account tramite la console SES:

1. Accedi alla AWS Management Console e apri la console Amazon SES all'indirizzo https://console.aws.amazon.com/ses/.
2. Nel pannello di navigazione, in Configuration (Configurazione) scegli Suppression list (Elenco di eliminazione).
3. Nel riquadro Suppression list (Elenco di eliminazione), seleziona la scheda Bulk actions (Operazioni in blocco).
4. Tutti i processi di importazione saranno elencati nella tabella Bulk actions (Operazioni in blocco) insieme al tipo di importazione, allo stato e alla data.
5. Per visualizzare i dettagli del processo, seleziona l'ID processo e verranno visualizzati i riquadri seguenti:

    a. Bulk action status (Stato operazione in blocco): mostra lo stato generale dei processi, l'ora e la data di completamento, il numero di record importati e il numero di record che non sono stati importati correttamente.

    b. Bulk action details (Dettagli operazione in blocco): mostra l'ID processo, indipendentemente dal fatto che sia stato utilizzato per aggiungere o rimuovere indirizzi, se il formato di file era JSON o CSV, l'URI del bucket Amazon S3 in cui è stato archiviato il file in blocco e l'ora e la data di creazione dell'operazione in blocco.

Disabilitazione dell'elenco di eliminazione a livello di account di Amazon SES

È possibile utilizzare il comando PutAccountSuppressionAttributes nell'API SES v2 per disabilitare in modo efficace l'elenco di eliminazione a livello di account rimuovendo i valori dall'attributo `suppressed-reasons`.

> **Note**
>
> La procedura seguente presuppone che sia già installata l'AWS CLI. Per ulteriori informazioni sull'installazione e la configurazione dell'AWS CLI, consulta la Guida per l'utente di AWS Command Line Interface.

Disabilitazione dell'elenco di eliminazione a livello di account utilizzando la AWS CLI

- Nella riga di comando, inserisci il comando seguente:

```
aws sesv2 put-account-suppression-attributes --suppressed-reasons
```

Disabilitazione dell'elenco di eliminazione a livello di account tramite la console SES:

1. Accedi alla AWS Management Console e apri la console Amazon SES all'indirizzo https://console.aws.amazon.com/ses/.
2. Nel pannello di navigazione, in Configuration (Configurazione) scegli Suppression list (Elenco di eliminazione).
3. Nel riquadro Account-level settings (Impostazioni a livello di account), scegliEdit (Modifica).
4. In Suppression list (Elenco di eliminazione), deseleziona la casella Enabled (Abilitato).
5. Seleziona Salva modifiche.

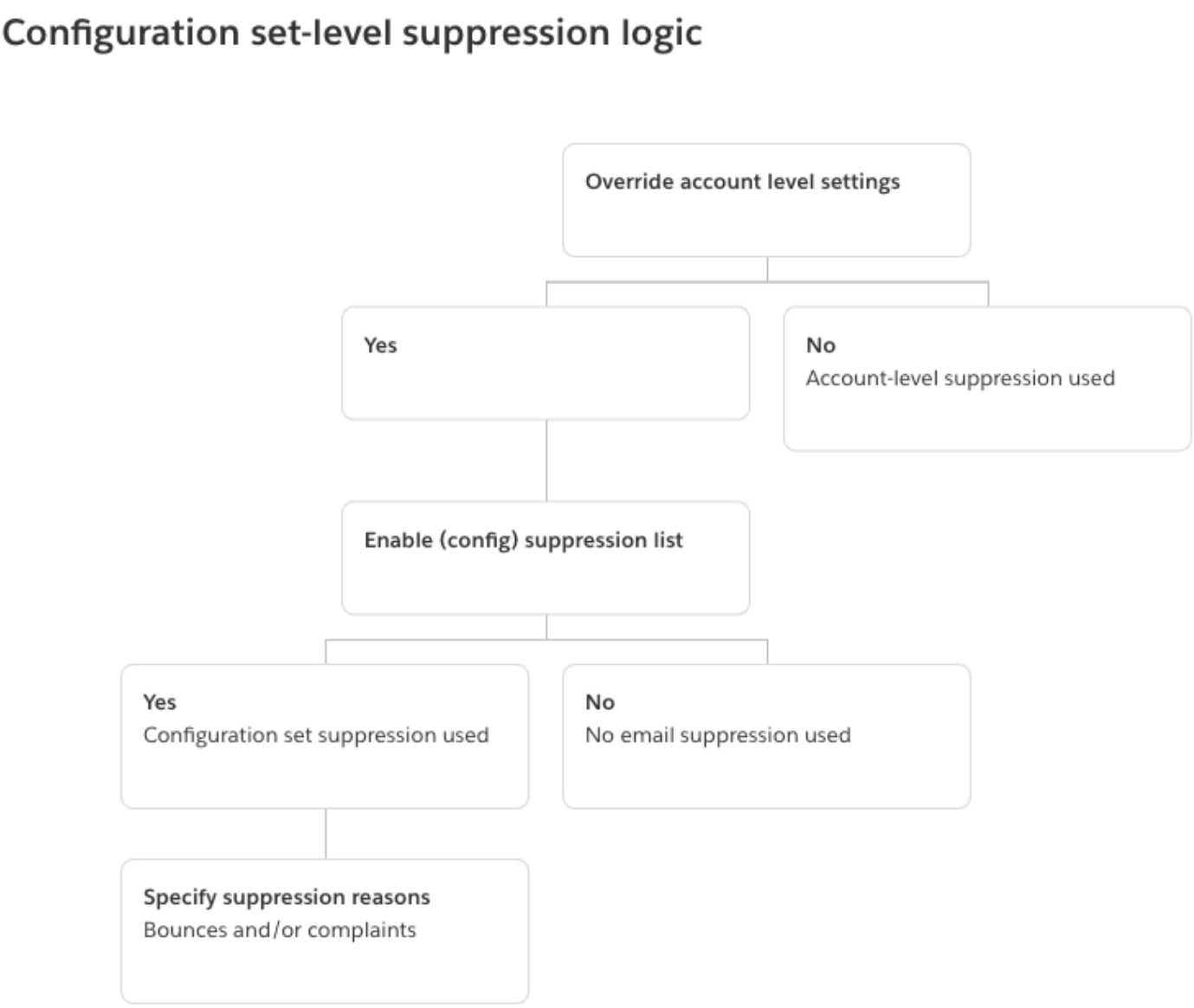
Utilizzo dell'eliminazione a livello di set di configurazione per ignorare l'elenco di eliminazione a livello di account

Mentre l'elenco di eliminazione a livello di account è impostato per l'intero account, puoi personalizzarlo separatamente per diversi set di configurazione sostituendolo con l'eliminazione a livello di set di configurazione. Questa granularità più precisa consente di utilizzare impostazioni di eliminazione personalizzate per diversi gruppi di invio e-mail assegnati ai propri set di configurazione. Ad esempio, supponiamo che l'elenco di eliminazione a livello di account sia configurato per l'aggiunta di indirizzi di mancato recapito e reclamo, ma in un set di configurazione è definito un determinato numero demografico di posta elettronica per il quale sei interessato solo all'aggiunta di indirizzi di reclamo. Puoi farlo abilitando le sostituzioni dell'eliminazione di set di configurazione in modo che gli indirizzi e-mail vengano aggiunti all'elenco di eliminazione a livello di account solo per reclami (non per mancati recapiti e reclami come è impostato nell'elenco di eliminazione a livello di account) dall'e-mail inviata con questo set di configurazione.

Con l'eliminazione a livello di set di configurazione, esistono diversi livelli di sovrascrittura dell'eliminazione a livello di account, incluso il non utilizzo dell'eliminazione. Per aiutare a comprendere questi diversi livelli di eliminazione che possono essere impostati nelle seguenti procedure della console, la seguente mappa delle relazioni modella il set decisionale di scelte

fatte per l'abilitazione o la disabilitazione di vari livelli di sovrascrittura, che a seconda della loro combinazione possono essere utilizzati per implementare tre diversi livelli di eliminazione:

- Nessuna sostituzione (impostazione predefinita) - il set di configurazione utilizza le impostazioni dell'elenco di eliminazione a livello di account.
- Ignora le impostazioni a livello di account - ciò annullerà qualsiasi impostazione dell'elenco di soppressione a livello di account; l'e-mail inviata con questo set di configurazione non utilizzerà alcuna impostazione di soppressione.
- Sostituisci le impostazioni a livello di account con l'eliminazione a livello di set di configurazione abilitata - l'e-mail inviata con questo set di configurazione utilizzerà solo le condizioni di eliminazione abilitate per questo (mancati recapiti, reclami o mancati recapiti e reclami); indipendentemente dalle impostazioni dell'elenco di eliminazione a livello di account, le sostituirà.



Non dimenticare che l'eliminazione a livello di set non è un elenco di eliminazione, piuttosto è un semplice meccanismo per sovrascrivere l'elenco di eliminazione a livello di account con impostazioni personalizzate dell'elenco di eliminazione definite in un set di configurazione. Questo significa che qualsiasi e-mail inviata utilizzando questo set di configurazione utilizzerà solo le proprie impostazioni di eliminazione e ignorerà le impostazioni di eliminazione a livello di account. In altre parole, l'eliminazione a livello di set di configurazione interagisce con l'elenco di soppressione a livello di account semplicemente modificando (ignorando) i motivi di eliminazione che determinano quali indirizzi e-mail vengono aggiunti all'elenco di eliminazione a livello di account.

Abilitazione dell'eliminazione a livello di set di configurazione

Per abilitare l'eliminazione a livello di set di configurazione utilizzando la nuova console di Amazon SES:

1. Accedere alla AWS Management Console e aprire la console Amazon SES all'indirizzo https://console.aws.amazon.com/ses/.
2. Nel pannello di navigazione, in Configuration (Configurazione), scegli Configuration sets (Set di configurazione).
3. In Configuration sets (Set di configurazione), scegli il nome del set di configurazione che vuoi configurare con l'eliminazione personalizzata.
4. Nel riquadro Suppression list options (Opzioni elenco di eliminazione), scegli Edit (Modifica).
5. La sezione Suppression list options (Opzioni elenco di eliminazione) fornisce un set di decisioni per definire l'eliminazione personalizzata a partire dall'opzione di utilizzare questo set di configurazione per sovrascrivere l'eliminazione a livello di account. La mappa logica di eliminazione a livello di set di configurazione ti aiuterà a comprendere gli effetti delle combinazioni di sovrascrittura. Queste selezioni su più livelli di sovrascrittura possono essere combinate per implementare tre diversi livelli di eliminazione:

   a. Use account-level suppression (Usa eliminazione a livello di account): non sovrascrivere l'eliminazione a livello di account e non implementare alcuna eliminazione a livello di set di configurazione. Fondamentalmente, qualsiasi e-mail inviata utilizzando questo set di configurazione utilizzerà solo l'eliminazione a livello di account. Per farlo:

      - In Suppression list settings (Impostazioni elenco di eliminazione), deseleziona la casella Override account level settings (Sovrascrivi impostazioni a livello di account).

   b. Do not use any suppression (Non usare alcuna eliminazione): sovrascrivi l'eliminazione a livello di account senza abilitare l'eliminazione a livello di set di configurazione. Questo significa che qualsiasi e-mail inviata utilizzando questo set di configurazione non utilizzerà alcuna eliminazione a livello di account. In altre parole, tutta l'eliminazione viene annullata. Per farlo:

      i. In Suppression list settings (Impostazioni elenco di eliminazione), controlla la casella Override account level settings (Sovrascrivi impostazioni a livello di account).

      ii. In Suppression list (Elenco di eliminazione), deseleziona la casella Enabled (Abilitato).

c. Usa eliminazione a livello di set di configurazione: sostituisci l'eliminazione a livello di account con impostazioni personalizzate dell'elenco di eliminazione definite in questo set di configurazione. Questo significa che qualsiasi e-mail inviata utilizzando questo set di configurazione utilizzerà solo le proprie impostazioni di eliminazione e ignorerà le impostazioni di eliminazione a livello di account. Per farlo:

   i. In Suppression list settings (Impostazioni elenco di eliminazione), controlla la casella Override account level settings (Sovrascrivi impostazioni a livello di account).

   ii. In Suppression list (Elenco di eliminazione), seleziona Enabled (Abilitato).

   iii. In Specify the reason(s)… (Specificare i motivi…), seleziona uno dei motivi dell'eliminazione da utilizzare per questo set di configurazione.

6. Scegliere Save changes (Salva modifiche).

Utilizzo della gestione degli elenchi

Amazon SES offre funzionalità di gestione degli elenchi, il che significa che i clienti possono gestire le proprie mailing list, note come liste di contatti. Un elenco di contatti è un elenco che consente di archiviare tutti i contatti che sono iscritti a uno o più argomenti specifici. Un contatto è un utente finale che riceve le tue email. Un argomento è un gruppo di interesse, un tema o un'etichetta all'interno di un elenco. Gli elenchi possono avere più argomenti.

Utilizzando il comando `ListContacts` nell'API Amazon SES v2, è possibile recuperare un elenco di tutti i contatti che si sono iscritti a un determinato argomento, ai quali è possibile inviare e-mail utilizzando il comando `SendEmail`.

Per informazioni sulla gestione delle sottoscrizioni, consulta Utilizzo della gestione delle sottoscrizioni.

Panoramica della gestione degli elenchi

Quando si utilizza la gestione elenchi, è necessario considerare i seguenti fattori:

- È possibile specificare gli argomenti dell'elenco durante la creazione dell'elenco.
- È consentito un solo elenco di contatti per Account AWS.
- Un elenco può avere un massimo di 20 argomenti.
- È possibile aggiornare un elenco contatti esistente, inclusi l'aggiunta di nuovi argomenti all'elenco, l'aggiunta o l'eliminazione di contatti da un elenco e l'aggiornamento delle preferenze dei contatti per un elenco o un argomento.

- È possibile aggiornare i metadati dell'argomento, ad esempio il nome visualizzato o la descrizione dell'argomento.
- È possibile ottenere un elenco di contatti in un elenco contatti, contatti sottoscritti a un argomento, contatti disiscritti da un argomento e contatti disiscritti da tutti gli argomenti dell'elenco.
- Puoi importare gli elenchi di contatti esistenti su Amazon SES utilizzando l'API `CreateImportJob`.
- Amazon SES non recapiterà un'e-mail se viene inviata a un contatto non iscritto nell'elenco dei contatti. Per ulteriori informazioni, consulta Utilizzo della gestione delle sottoscrizioni.
- Ogni contatto può avere attributi associati che è possibile utilizzare per memorizzare informazioni su quel contatto.

Configurazione della gestione degli elenchi

È possibile utilizzare le seguenti operazioni di seguenti per configurare le funzionalità di gestione degli elenchi. Per l'elenco completo dell'elenco dei contatti e delle operazioni dei contatti, consulta il Documento di riferimento all'API Amazon SES v2.

Creazione di un elenco di contatti

Puoi utilizzare il comando `CreateContactList` nell'API Amazon SES v2 per creare un elenco di contatti. Puoi configurare rapidamente e facilmente questa impostazione utilizzando l'AWS CLI. Per ulteriori informazioni sull'installazione e la configurazione dell'AWS CLI, consulta la Guida per l'utente di AWS Command Line Interface.

Creazione di un elenco di contatti mediante l'AWS CLI

- Nella riga di comando, inserisci il comando seguente:

```
aws sesv2 create-contact-list --cli-input-json file://CONTACT-LIST-JSON
```

Nel precedente comando, sostituire *CONTACT-LIST-JSON* con il percorso del file JSON per la richiesta `CreateContactList`.

Un esempio di file JSON di input `CreateContactList` per la richiesta è il seguente:

```
{
    "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"
    }
   ]
}
```

Creazione di un contatto

Puoi utilizzare il comando `CreateContact` nell'API Amazon SES v2 per creare un contatto. Puoi configurare rapidamente e facilmente questa impostazione utilizzando l'AWS CLI. Per ulteriori informazioni sull'installazione e la configurazione dell'AWS CLI, consulta la Guida per l'utente di AWS Command Line Interface.

Creazione di un contatto mediante l'AWS CLI

- Nella riga di comando, inserisci il comando seguente:

```
aws sesv2 create-contact --cli-input-json file://CONTACT-JSON
```

Nel precedente comando, sostituire *CONTACT-JSON* con il percorso del file JSON per la richiesta `CreateContact`.

Un esempio di file JSON di input `CreateContact` per la richiesta è il seguente:

```
{
    "ContactListName": "ExampleContactListName",
    "EmailAddress": "example@amazon.com",
    "UnsubscribeAll": false,
    "TopicPreferences": [
        {
            "TopicName": "Sports",
            "SubscriptionStatus": "OPT_IN"
        }
    ],
    "AttributesData": "{\"Name\": \"John\", \"Location\": \"Seattle\"}"
}
```

Nell'esempio precedente, un valore `UnsubscribeAll` di `false` indica che il contatto non ha annullato la sottoscrizione a tutti gli argomenti, laddove un valore di `true` significherebbe che il contatto ha annullato la sottoscrizione a tutti gli argomenti.

`TopicPreferences` include informazioni sullo stato della sottoscrizione del contatto agli argomenti. Nell'esempio precedente, il contatto ha scelto l'argomento "Sports" e riceverà tutti i messaggi di posta elettronica relativi all'argomento "Sports".

`AttributesData` è un campo JSON in cui è possibile inserire qualsiasi tipo di metadati sul nostro contatto. Deve essere un oggetto JSON valido.

Importazione in blocco dei contatti nell'elenco di contatti

Puoi aggiungere manualmente gli indirizzi in blocco caricando prima i contatti in un oggetto Simple Storage Service (Amazon S3), seguito dall'operazione `CreateImportJob` nell'API Amazon SES v2 o utilizzando la console SES. Per ulteriori informazioni, consulta Aggiunta di indirizzi e-mail in blocco all'elenco di eliminazione a livello di account.

È necessario creare un elenco di contatti prima di importare i contatti.

> **Note**
>
> È possibile aggiungere fino a 1 milione di contatti a un elenco di contatti per ImportJob.

Per aggiungere contatti in blocco all'elenco di contatti, procedere come segue.

- Carica i tuoi contatti in un oggetto Amazon S3 in formato CSV o JSON.

  Formato CSV

  La prima riga del file che viene caricato su Amazon S3 dovrebbe essere una riga di intestazione.

  L'oggetto `topicPreferences` deve essere appiattito per il formato CSV. Ogni argomento in `topicPreferences` avrà un campo di intestazione separato.

  Esempio di formato CSV per l'aggiunta di contatti in blocco a un elenco di contatti:

```
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

  Sono supportati solo i file JSON delimitati da nuova riga. In questo formato, ogni riga è un oggetto JSON completo che contiene le informazioni di un contatto.

  Esempio di formato JSON per l'aggiunta di contatti in blocco a un elenco di contatti:

```
{
     "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"
        }
      ]
}
```

Negli esempi precedenti, sostituire *example1@amazon.com* ed *example2@amazon.com* con gli indirizzi e-mail che si desidera aggiungere all'elenco di contatti. Sostituire i valori `attributesData` con i valori specifici del contatto. Inoltre, sostituire *Sports* e *Cycling* con `topicName` che si applica al contatto. Le `topicPreferences` accettabili sono *OPT_IN* e *OPT_OUT*.

I seguenti attributi sono supportati durante il caricamento dei contatti in un oggetto Simple Storage Service (Amazon S3) in formato CSV o JSON:

Attributo	Descrizione
`emailAddress`	L'indirizzo email del contatto. Questo è un campo obbligatorio.
`unsubscribeAll`	Uno stato di valore booleano che indica se il contatto è disiscritto da tutti gli argomenti dell'elenco di contatti.

Attributo	Descrizione
`topicPreferences`	Preferenze del contatto per l'accettazione o l'esclusione degli argomenti.
`attributesData`	Dati degli attributi allegati a un contatto.

- Consente ad Amazon SES l'autorizzazione a leggere l'oggetto Amazon S3.

  Se applicata a un bucket Amazon S3, la seguente policy concede ad Amazon SES l'autorizzazione a leggere tale bucket. Per maggiori informazioni sulle policy dei bucket per Amazon S3, consulta Utilizzo delle policy dei bucket e dell'utente nella Guida per l'utente di 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"
                }
            }
        }
    ]
}
```

- Concede ad Amazon SES l'autorizzazione a utilizzare la chiave AWS KMS.

  Se l'oggetto Amazon S3 è crittografato con una chiave AWS KMS, devi concedere ad Amazon SES l'autorizzazione necessaria per utilizzare la chiave KMS. Amazon SES può ottenere l'autorizzazione solo da una chiave gestita dal cliente, non da una chiave KMS predefinita. Devi concedere ad Amazon SES l'autorizzazione a utilizzare la chiave gestita dal cliente aggiungendo un'istruzione alla policy della chiave.

Incolla la seguente istruzione nella policy della chiave per consentire ad Amazon SES di utilizzare la tua chiave gestita dal cliente.

```
{
   "Sid": "AllowSESToDecrypt",
   "Effect": "Allow",
   "Principal": {
       "Service":"ses.amazonaws.com"
   },
   "Action": [
       "kms:Decrypt",
   ],
   "Resource": "*"
}
```

- Utilizzare il comando `CreateImportJob` nell'API Amazon SES v2.

> **Note**
>
> L'esempio seguente presuppone che sia già installata l'AWS CLI. Per ulteriori informazioni sull'installazione e la configurazione dell'AWS CLI, consulta la Guida per l'utente di AWS Command Line Interface.

Nella riga di comando, immetti il comando seguente: Sostituire *`s3bucket`* con il nome del bucket Amazon S3 e *`s3object`* con il nome dell'oggetto Amazon S3.

```
aws sesv2 create-import-job --import-destination
 ContactListDestination={ContactListName=ExampleContactListName,ContactListImportAction=PUT}
 --import-data-source S3Url="s3://s3bucket/s3object",DataFormat=CSV
```

Procedura dettagliata per la gestione degli elenchi con esempi

La seguente procedura dettagliata fornisce esempi di come utilizzare la gestione degli elenchi per elencare i contatti, utilizzare`ListManagementOptions` per specificare un elenco di contatti e il nome dell'argomento nell'e-mail e come inserire i collegamenti di annullamento della sottoscrizione.

1. Elencare i contatti mediante l'AWS CLI: utilizzando il comando `ListContacts` è possibile recuperare un elenco di tutti i contatti che si sono iscritti a un determinato argomento, insieme al comando `SendEmail` che consente di inviare loro e-mail.

   Nella riga di comando, inserisci il comando seguente:

   ```
   aws sesv2 list-contacts --cli-input-json file://LIST-CONTACTS-JSON
   ```

   Nel precedente comando, sostituire *`LIST-CONTACTS-JSON`* con il percorso al file JSON per la richiesta `ListContacts`.

   Un esempio di file JSON di input `ListContacts` per la richiesta è il seguente:

   ```
   {
       "ContactListName": "ExampleContactListName",
       "Filter": {
           "FilteredStatus": "OPT_IN",
           "TopicFilter": {
               "TopicName": "Cycling",
               "UseDefaultIfPreferenceUnavailable": true
           }
       },
       "PageSize": 50
   }
   ```

   `FilteredStatus` mostra lo stato della sottoscrizione per il quale si desidera filtrare, ovvero `OPT_IN` o `OPT_OUT`.

   `TopicFilter` è un filtro facoltativo che specifica l'argomento per cui si desidera ottenere risultati e, nell'esempio precedente, è "Cycling".

   `UseDefaultIfPreferenceUnavailable` può avere un valore di `true` o `false`. Se `true`, verrà utilizzata la preferenza predefinita dell'argomento se il contatto non dispone di alcuna preferenza esplicita per un argomento. Se `false`, solo i contatti con una preferenza impostata esplicitamente vengono considerati per il filtraggio.

2. Invia posta con **`ListManagementOptions`** abilitato: dopo aver elencato i contatti nell'elenco utilizzando il precedente comando `ListContacts`, è possibile utilizzare il comando `SendEmail` per inviare e-mail a ciascun contatto utilizzando l'intestazione `ListManagementOptions` per specificare l'elenco dei contatti e il nome dell'argomento.

Per utilizzare `ListManagementOptions` con il comando `SendEmail`, includere `contactListName` e `topicName` a cui appartiene l'e-mail (`topicName` è facoltativo):

```
ListManagementOptions:
    String contactListName
    String topicName
```

Se includi `ListManagementOptions` nella richiesta `SendEmail` a un indirizzo e-mail del destinatario che non è presente nell'elenco dei contatti, verrà creato automaticamente un contatto nell'elenco.

Amazon SES non recapiterà un'e-mail se viene inviata a un contatto non iscritto nell'elenco dei contatti, il che significa che non dovrai aggiornare le richieste `SendEmail` per evitare l'invio a contatti che hanno annullato la sottoscrizione.

3. Indicare la posizione per i collegamenti di annullamento della sottoscrizione: quando si utilizza `ListManagementOptions` hai la possibilità di abilitare Amazon SES di aggiungere collegamenti a piè di pagina di annullamento della sottoscrizione nella tua e-mail utilizzando il placeholder `{{amazonSESUnsubscribeUrl}}` per specificare dove SES deve inserire l'URL di annullamento della sottoscrizione. La sostituzione dei placeholder è supportata solo per i tipi di contenuto HTML e TEXT. È possibile includere il placeholder al massimo due volte. Se usato più di due volte, vengono sostituite solo le prime due occorrenze. Per ulteriori informazioni, consulta Utilizzo della gestione delle sottoscrizioni.

   In alternativa, puoi utilizzare l'intestazione `X-SES-LIST-MANAGEMENT-OPTIONS` per specificare un elenco e un nome di argomento durante l'invio di e-mail utilizzando l'interfaccia SMTP.

   Per specificare il nome di un elenco e di un argomento durante l'invio di e-mail utilizzando l'interfaccia SMTP, aggiungere la seguente intestazione di posta elettronica al messaggio:

   ```
   X-SES-LIST-MANAGEMENT-OPTIONS: {contactListName}; topic={topicName}
   ```

Utilizzo della gestione delle sottoscrizioni

Amazon SES fornisce una funzionalità di gestione delle sottoscrizioni, in cui Amazon SES abilita automaticamente i collegamenti di annullamento della sottoscrizione in ogni e-mail in uscita quando

si specificano `contactListName` e `topicName` in `ListManagementOptions` nella richiesta del comando `SendEmail`.

Se un contatto annulla la sottoscrizione a un determinato argomento o elenco, Amazon SES non consente l'invio di e-mail al contatto per tale argomento o elenco in futuro.

> **Note**
>
> - La gestione degli abbonamenti Amazon SES supporta i requisiti per mittenti in blocco, come richiesto da molti provider di servizi di posta elettronica. Per ulteriori informazioni, consulta la Sezione 2 in Panoramica delle modifiche in blocco dei mittenti.
> - La gestione delle sottoscrizioni è disponibile per coloro che utilizzano Easy DKIM in Amazon SES, ma Amazon SES non permette di aggiungere i collegamenti di annullamento dell'iscrizione alla tua e-mail per i mittenti che firmano personalmente le email prima di chiamare Amazon SES.

Per informazioni sulla gestione degli elenchi e su come utilizzarla, incluso il recupero di un elenco di tutti i contatti che hanno effettuato la sottoscrizione a un determinato argomento, consulta Utilizzo della gestione degli elenchi.

Panoramica della gestione delle sottoscrizioni

Quando si utilizza la gestione delle sottoscrizioni, è necessario considerare i seguenti fattori:

- La gestione delle sottoscrizioni è eseguita in modo automatico da Amazon SES. Ciò significa che Amazon SES riceve e-mail e richieste di annullamento dell'iscrizione dalla pagina Web di disiscrizione e aggiorna le preferenze del contatto nel tuo elenco. È possibile ricevere notifiche di annullamento della sottoscrizione utilizzando le notifiche dei set di configurazione. Per ulteriori informazioni sui set di configurazione, consulta Utilizzo dei set di configurazione in Amazon SES.
- È necessario specificare l'elenco di contatti durante l'invio dell'e-mail. La gestione delle sottoscrizioni tramite i collegamenti di intestazione `List-Unsubscribe` e di piè di pagina `ListManagementOptions` verrà gestita di conseguenza.
- Amazon SES aggiunge il supporto per gli standard di intestazione `List-Unsubscribe`, che consentono ai client e-mail e ai provider di posta in arrivo di visualizzare un collegamento di annullamento della sottoscrizione nella parte superiore dell'e-mail, se sono supportate le intestazioni. Non tutti i fornitori di servizi supportano tali intestazioni.

- Le intestazioni `List-Unsubscribe` seguono il seguente comportamento:
  - Se un contatto fa clic sul collegamento di annullamento della sottoscrizione in un'e-mail contenente sia l'elenco contatti che l'argomento specificati, l'annullamento della sottoscrizione del contatto avverrà solo da tale argomento specifico.
  - Se l'argomento non è specificato, il contatto verrà disiscritto da tutti gli argomenti dell'elenco.
- I contatti verranno indirizzati a una pagina di destinazione per annullare l'iscrizione quando fanno clic su un collegamento di annullamento della sottoscrizione nel piè di pagina dell'e-mail.
- La pagina di destinazione di annullamento dell'iscrizione darà ai contatti un'opzione per aggiornare le loro preferenze, ovvero `OPT_IN` o `OPT_OUT`, per tutti gli argomenti di un particolare elenco. La pagina di destinazione offre inoltre la possibilità di annullare l'iscrizione a tutti gli argomenti dell'elenco.
- Se utilizzi `ListManagementOptions`, devi includere un placeholder `{{amazonSESUnsubscribeUrl}}` nelle tue e-mail per indicare dove Amazon SES deve inserire l'URL di annullamento della sottoscrizione. È possibile includere il placeholder al massimo due volte. Se usato più di due volte, vengono sostituite solo le prime due occorrenze.
- I collegamenti di intestazione `List-Unsubscribe` e di piè di pagina `ListManagementOptions` vengono aggiunti solo se l'e-mail viene inviata a un singolo destinatario.
- Per le e-mail transazionali in cui non si desidera che i contatti siano in grado di annullare la sottoscrizione, è possibile omettere il campo `ListManagementOptions` con la propria richiesta `SendEmail`.

Considerazioni sull'intestazione di annullamento della sottoscrizione

La gestione delle sottoscrizioni tramite un collegamento di annullamento della sottoscrizione è abilitata quando l'e-mail contiene le seguenti intestazioni:

`List-Unsubscribe`

`List-Unsubscribe-Post`

Quando utilizzi la gestione delle sottoscrizioni di Amazon SES `ListManagementOptions`, Amazon SES sostituirà queste intestazioni se sono presenti nell'e-mail.

I destinatari che annullano la sottoscrizione facendo clic sul collegamento prodotto da queste intestazioni avranno un'esperienza diversa a seconda del client e-mail o del provider di posta in arrivo perché alcuni provider non riconoscono le intestazioni `List-Unsubscribe` e `List-Unsubscribe-`

`Post`; l'e-mail inviata ai destinatari utilizzando tali provider non visualizzerà il collegamento di annullamento della sottoscrizione.

I destinatari il cui client e-mail riconosce queste intestazioni visualizzeranno il collegamento di annullamento della sottoscrizione e potranno annullarla tramite il collegamento, ma non avranno la possibilità di scegliere di quali argomenti annullare la sottoscrizione. L'annullamento della sottoscrizione avverrà semplicemente dall'argomento a cui è stata inviata l'e-mail.

Per ulteriori informazioni sull'intestazione `List-Unsubscribe`, consulta RFC 2369 e per l'intestazione `List-Unsubscribe-Post`, consulta RFC 8058.

> **Note**
>
> Amazon SES supporta l'annullamento dell'iscrizione con un clic in conformità ai requisiti Bulk Sender imposti da molti provider di servizi di posta elettronica. Per ulteriori informazioni, consulta la sezione Utilizzo dell'annullamento dell'iscrizione con un clic con Amazon SES.

Aggiungere un collegamento per annullare la sottoscrizione nel piè di pagina

È necessario utilizzare il placeholder `{{amazonSESUnsubscribeUrl}}` nelle e-mail preimpostate e non per specificare dove Amazon SES deve inserire l'URL di annullamento dell'iscrizione.

La sostituzione dei placeholder è supportata solo per i tipi di contenuto HTML e TEXT.

È possibile includere il placeholder al massimo due volte. Se usato più di due volte, vengono sostituite solo le prime due occorrenze.

> **Note**
>
> Il placeholder `{{amazonSESUnsubscribeUrl}}` può essere utilizzato solo `ListManagementOptions` se è specificato come intestazione durante l'utilizzo del comando `SendEmail`o se X-SES-LIST-MANAGEMENT-OPTIONS viene specificato come intestazione durante l'utilizzo dell'interfaccia SMTP. (Da non confondere con le intestazione `List-Unsubscribe` o `List-Unsubscribe-Post` che non dipendono da `ListManagementOptions` e possono essere utilizzate singolarmente.)

Monitoraggio delle attività di invio di Amazon SES

Amazon SES fornisce metodi per monitorare le attività di invio utilizzando eventi, parametri e statistiche. Un evento è qualcosa che accade correlato alla tua attività di invio di cui ne hai specificato il monitoraggio come parametro. Un parametro rappresenta un set di punti dati ordinato in base al tempo che rappresenta i valori di un tipo di evento monitorato che produce statistiche. Le statistiche sono aggregazioni di dati di parametri per un periodo di tempo specificato fino ad oggi.

Questi metodi di monitoraggio aiutano a tenere traccia di misure importanti, come le percentuali di mancati recapiti, reclami e rifiuti. Percentuali troppo alte di mancati recapiti e reclami possono compromettere la tua capacità di inviare e-mail utilizzando SES. Questi metodi possono anche essere utilizzati per misurare le percentuali con cui i clienti interagiscono con le e-mail inviate aiutandoti a identificare le percentuali complessive di apertura e di clic attraverso la pubblicazione degli eventi e i domini personalizzati associati ai set di configurazione; consulta Configurazione di domini personalizzati per gestire il monitoraggio di aperture e clic.

Il primo passo per configurare il monitoraggio consiste nell'identificare i tipi di eventi dell'e-mail relativi all'attività di invio che desideri misurare e monitorare utilizzando SES. Puoi scegliere i seguenti tipi di evento da monitorare in SES:

- Send (Invio): la richiesta di invio è stata completata e Amazon SES tenterà la consegna del messaggio al server di posta del destinatario. Se viene utilizzata l'eliminazione globale o a livello di account, SES la conteggia comunque come invio, ma la consegna viene eliminata.
- RenderingFailure— L'e-mail non è stata inviata a causa di un problema di rendering del modello. Questo tipo di evento può verificarsi se i dati del modello mancano o se non vi è corrispondenza tra i parametri e i dati del modello. Questo tipo di evento si verifica solo quando invii un'e-mail basata su modello utilizzando le operazioni API `SendTemplatedEmail` o `SendBulkTemplatedEmail`.
- Reject (Rifiuta): Amazon SES ha accettato l'e-mail, ma ha stabilito che conteneva un virus e non ha tentato di consegnarla al server di posta del destinatario.
- Delivery (Consegna): Amazon SES ha consegnato correttamente l'e-mail al server di posta del destinatario.
- Mancato recapito: un mancato recapito permanente indica che il server di posta del destinatario ha rifiutato l'e-mail in modo permanente. (I casi di soft bounce (e-mail non recapitata) sono previsti solo se Amazon SES non riesce a inviare il messaggio e-mail dopo avere ritentato per un determinato periodo di tempo).

- Complaint (Reclamo): l'e-mail è stata recapitata correttamente al server di posta del destinatario, ma il destinatario l'ha contrassegnata come spam.
- DeliveryDelay— L'e-mail non può essere recapitata al server di posta del destinatario a causa di un problema temporaneo. I ritardi di consegna possono verificarsi, ad esempio quando la casella di posta in arrivo del destinatario è piena o quando nel server di ricezione della posta elettronica si verifica un problema transitorio.
- Subscription (Sottoscrizione): l'e-mail è stata recapitata correttamente, ma il destinatario ha aggiornato le preferenze di sottoscrizione facendo clic su `List-Unsubscribe` nell'intestazione dell'email o sul collegamento `Unsubscribe` nel piè di pagina.
- Open (Apri): il destinatario ha ricevuto il messaggio e lo ha aperto nel proprio client e-mail.
- Click (Clic): il destinatario ha fatto clic su uno o più collegamenti contenuti nell'e-mail.

Puoi monitorare gli eventi di invio di e-mail in vari modi. Il metodo di monitoraggio che scegli dipende dal tipo di evento che desideri monitorare, dalla granularità e dal livello di dettaglio con il quale desideri monitorarlo e la posizione da dove desideri che Amazon SES pubblichi i dati. Devi utilizzare un feedback di notifica o la pubblicazione di eventi per tenere traccia degli eventi di mancato recapito e reclamo. Puoi inoltre scegliere di utilizzare più metodi di monitoraggio. Le caratteristiche di ciascun metodo sono elencate nella seguente tabella.

Metodo di monitoraggio	Eventi che puoi monitorare	Modalità di accesso ai dati	Livello di dettaglio	Granularity (Granularità)
Console Amazon SES	Stato dell'account, e-mail inviate, quota utilizzata, richieste di invio andate a buon fine, rifiuti, mancati recapiti e reclami (storia recente fino alla reputazione attuale)	Pagina del pannello di controllo dell'account nella console Amazon SES	Conteggio e percentuale	In tutto l'account AWS

Metodo di monitoraggio	Eventi che puoi monitorare	Modalità di accesso ai dati	Livello di dettaglio	Granularity (Granularità)
Console Amazon SES	Stato dell'account, e-mail inviate, mancati recapiti e reclami (reputazione attuale)	Pagina dei parametri di reputazione nella console Amazon SES	Solo percentuali calcolate	In tutto l'account AWS
API Amazon SES	Consegne, mancati recapiti, reclami e rifiuti	Operazione API `GetSendStatistics`	Solo conteggio	In tutto l'account AWS

Metodo di monitoraggio	Eventi che puoi monitorare	Modalità di accesso ai dati	Livello di dettaglio	Granularity (Granularità)
CloudWatch Console Amazon	Invii, consegne, aperture, clic, mancati recapiti, frequenza di mancati recapiti, reclami, percentuale di reclami rifiuti, errori di rendering e IP inseriti in blacklist.	CloudWatch console **Note** Alcune metriche non vengono visualizzate CloudWatch finché non si verifica l'evento associato. Ad esempio, le metriche di rimbalzo non vengono visualizzate CloudWatch fino a quando non invii almeno un'email o finché	Solo conteggio	In tutto l'account AWS

Metodo di monitoraggio	Eventi che puoi monitorare	Modalità di accesso ai dati	Livello di dettaglio	Granularity (Granularità)
		non generi un evento di rimbalzo simulato utilizzando il simulatore di caselle di posta.		
Notifiche di feedback	Consegne, mancati recapiti e reclami	Notifica di Amazon SNS (consegne, mancati recapiti e reclami) o e-mail (solo mancati recapiti e reclami). Per informazioni, consulta Impostazione della notifica di eventi.	Dettagli su ogni evento	In tutto l'account AWS

Metodo di monitoraggio	Eventi che puoi monitorare	Modalità di accesso ai dati	Livello di dettaglio	Granularity (Granularità)
Event publishing (Pubblicazione degli eventi)	Invii, consegne, aperture, clic, mancati recapiti, reclami, rifiuti ed errori di rendering	Amazon CloudWatch o Amazon Data Firehose o tramite notifica Amazon SNS: vedi. Monitoraggio dell'invio di e-mail utilizzando la pubblicazione di eventi (Si applicano costi aggiuntivi, vedi Prezzo per metrica per.) CloudWatch	Dettagli su ogni evento	Granulare (in base alle caratteristiche e-mail definibili dall'utente)
Pubblicazione degli eventi utilizzando domini personalizzati associati ai set di configurazione: ulteriori informazioni	Monitoraggio di apertura e di clic.	Amazon CloudWatch o Amazon Data Firehose o tramite notifica Amazon SNS. (Si applicano costi aggiuntivi, consulta Prezzo per metrica per.) CloudWatch	Dettagli su ogni evento.	Granulare (in base alle caratteristiche e-mail definibili dall'utente)

> **Note**
>
> I parametri misurati dagli eventi di invio di e-mail potrebbero non allinearsi perfettamente con le quote di invio. Questa discrepanza può essere causata da mancati recapiti e rifiuti oppure dall'uso del simulatore di mailbox Amazon SES. Per vedere quanto manca al raggiungimento delle quote di invio, consulta Monitoraggio delle quote di invio.

Per informazioni su come utilizzare ciascun metodo di monitoraggio, consulta i seguenti argomenti:

- Monitoraggio delle statistiche di invio utilizzando la console Amazon SES
- Monitoraggio delle statistiche di utilizzo tramite l'API Amazon SES
- Monitoraggio dell'invio di e-mail utilizzando la pubblicazione di eventi di Amazon SES

Monitoraggio delle statistiche di invio utilizzando la console Amazon SES

Nelle pagine Dashboard dell'account, Parametri di reputazione e Impostazioni SMTP della console Amazon SES è possibile monitorare l'invio di email, l'utilizzo, le statistiche, le impostazioni SMTP e lo stato generale dell'account e i parametri di reputazione. Nelle sezioni seguenti vengono descritti i parametri e le statistiche fornite in ciascuna di queste pagine della console.

Va notato che mentre entrambe le pagine della console the section called “Pannello di controllo account” e the section called “Parametri di reputazione” contengono parametri di mancato recapito e reclami, c'è una sottile differenza tra questi due set di percentuali di mancato recapito e di reclami come illustrato di seguito:

- Pagina Account dashboard (Pannello di controllo account): in base all'intervallo di date selezionato, puoi visualizzare quali erano le percentuali di mancati recapiti e reclami in passato con la progressione dei cambiamenti del parametro fino ad oggi.
- Pagina Reputation metrics (Parametri di reputazione): percentuali di mancato recapito e di reclami in base all'ultimo punto dati ricevuto dal calcolo della media storica complessiva a un livello elevato (da non confondere con la frequenza di mancato recapito/reclamo regolare, che corrisponde a precisi eventi di mancato recapito/reclamo nel momento in cui si verificano in tempo reale, come mostrato nella pagina Account dashboard (Pannello di controllo account).

Come semplice esempio per confrontare le percentuali di mancato recapito o di reclamo tra la pagina Reputation metrics (Parametri di reputazione) e la pagina Account dashboard (Pannello di controllo account), supponiamo che la percentuale fosse del 2% ieri ed è dell'1% ora; nella pagina Reputation metrics (Parametri di reputazione), verrà visualizzata solo la percentuale corrente dell'1%, ma nella pagina Account dashboard (Pannello di controllo account), i grafici tracceranno la progressione che mostra una percentuale del 2% per ieri e dell'1% per oggi.

Pannello di controllo account

È possibile monitorare il numero di e-mail inviate dal proprio account, nonché la percentuale di quota di invio che è stata utilizzata, direttamente dalla pagina Account dashboard (Pannello di controllo account) della console Amazon SES nel riquadro Daily email usage (Utilizzo giornaliero di e-mail). Le percentuali di consegne e di rifiuti per l'account possono essere monitorate nel riquadro Sending Statistics (Statistiche di invio), insieme ad altri fattori chiave relativi all'invio di e-mail nei seguenti riquadri:

- Limiti di invio: contiene le seguenti quote applicabili all'invio di e-mail tramite SES:
  - Quota di invio giornaliera: il numero massimo di e-mail che è possibile inviare in un periodo di tempo di 24 ore.
  - Frequenza massima di invio: il numero massimo di e-mail al secondo che è possibile inviare dall'account.
- Integrità dell'account - lo stato del tuo account SES:
  - `Healthy` - non ci sono problemi legati alla reputazione che attualmente influiscono sul tuo account.
  - `Under review` - sono stati identificati potenziali problemi con il tuo account SES - il tuo account è in fase di revisione mentre lavori per correggere i problemi.
  - `Paused` - la capacità del tuo account di inviare e-mail è attualmente sospesa a causa di un problema con l'e-mail inviata dal tuo account. Quando il problema è stato corretto, puoi richiedere che la capacità del tuo account di inviare e-mail venga ripresa.
- Utilizzo giornaliero dell'e-mail - per verificare il tuo utilizzo quotidiano per assicurarti di non avvicinarti ai limiti di invio:
  - Email inviate: numero totale di e-mail inviate in un periodo di tempo di 24 ore.
  - Invii restanti: numero totale di e-mail restanti disponibili per l'invio in un periodo di tempo di 24 ore.
  - Quota di invio utilizzata: percentuale della quota di invio giornaliera utilizzata.

- Statistiche di invio - è composta da grafici che mostrano la progressione di quattro parametri essenziali in un insieme di punti dati ordinati in base al tempo che rappresentano i valori di un tipo di evento monitorato che produce statistiche per l'intervallo di date selezionato utilizzando un periodo di aggregazione di 1 ora. Puoi selezionare un intervallo di date con valori iniziali da `Last 1 day` a `Last 14 days` per filtrare i grafici riportati di seguito:
  - Invii: la somma delle richieste di invio e-mail andate a buon fine per l'intervallo di date selezionato.
  - Rifiuti: percentuale media delle richieste di invio rifiutate da parte di SES in base a `Rejects/Sends * 100` per l'intervallo di date selezionato.
  - Mancati recapiti: percentuale media ricavata dai parametri di reputazione cronologici complessivi del mittente che mostrano la progressione per l'intervallo di date selezionato.
  - Reclami: percentuale media ricavata dai parametri di reputazione cronologici complessivi del mittente che mostrano la progressione per l'intervallo di date selezionato.

Ognuno di questi grafici contiene un pulsante View in CloudWatch (Visualizza in CloudWatch) che apre il rispettivo parametro nella console Amazon CloudWatch permettendo di visualizzare dati dettagliati, eseguire calcoli personalizzati dei parametri e creare allarmi in CloudWatch.

Parametri di reputazione

Oltre alle percentuali di mancato recapito e di reclami, la pagina Reputation metrics (Parametri di reputazione) fornisce anche ulteriore visibilità di alto livello sui fattori chiave che influenzano la reputazione nei seguenti riquadri:

- Riepilogo: fornisce una panoramica della stato della tua reputazione.
  - Stato: stato generale della reputazione basata sulle percentuali di mancato recapito e reclamo cronologiche:
    - `Healthy` - entrambi i parametri sono all'interno di livelli normali.
    - `Under review` - uno o entrambi i parametri hanno automaticamente causato la messa in fase di verifica dell'account.
    - `At risk` - uno o entrambi i parametri hanno raggiunto livelli malsani e la capacità del tuo account di inviare e-mail potrebbe essere a rischio.
  - Email inviate (ultime 24 ore): numero totale di e-mail inviate in un periodo di tempo di 24 ore.
  - Invii restanti: numero totale di e-mail restanti disponibili per l'invio in un periodo di tempo di 24 ore.

    - Quota di invio utilizzata: percentuale della quota di invio giornaliera utilizzata.
- Contenuto della scheda a livello di account:
    - Bounce rate (Percentuale di mancati recapiti (bounce))
        - Stato: indica lo stato della frequenza di mancato recapito utilizzando gli stessi valori descritti per il riquadro Summary (Riepilogo).
        - Frequenza di mancato recapito cronologica: percentuale di e-mail dal proprio account che ha determinato un mancato recapito permanente calcolato dalla media cronologica complessiva in base a un volume rappresentativo che rappresenta le pratiche di invio tipiche.
    - Complaint rate (Percentuale di reclami)
        - Stato: indica lo stato della percentuale di reclami utilizzando gli stessi valori descritti per il riquadro Summary (Riepilogo).
        - Percentuale di mancato recapito cronologica: percentuale di e-mail inviate dal proprio account che i destinatari hanno segnalato come spam calcolata sulla base della media cronologica complessiva in base a un volume rappresentativo che rappresenta le pratiche di invio tipiche.
- Contenuto della scheda del set di configurazione:
    - Reputazione per set di configurazione
        - Set di configurazione: consente di digitare o selezionare un set di configurazione con parametri di reputazione abilitati per visualizzare i dati di riepilogo, mancato recapito e reclamo in base alle e-mail inviate utilizzando il set di configurazione selezionato. I pannelli risultanti che vengono visualizzati dopo aver selezionato un set di configurazione sono gli stessi descritti sopra per la pagina di parametri Reputazione, tranne che si basano solo sull'e-mail inviata con il set di configurazione selezionato e non sui parametri complessivi di invio a livello di account.

Impostazioni SMTP

In questa pagina sono elencate le impostazioni SMTP necessarie per utilizzare l'interfaccia SMTP di Amazon SES tramite l'API SES o a livello di programmazione, assieme ai collegamenti per la creazione e la gestione delle credenziali SMTP.

- Impostazioni SMTP - se desideri utilizzare linguaggi di programmazione, server e-mail o applicazione compatibili con SMTP per connettersi all'interfaccia SMTP di Amazon SES, vengono fornite le seguenti informazioni:
    - SMTP endpoint
    - STARTTLS Porta

- Transport Layer Security (TLS)
- TLS Wrapper Porta
- Collegamenti di autenticazione forniti per la creazione e la gestione delle credenziali SMTP e IAM

Utilizzo della console per monitorare i parametri di invio e di reputazione

Le seguenti procedure consentiranno di iniziare a esplorare i propri parametri di invio e reputazione utilizzando la pagina Account dashboard (Pannello di controllo account) per i parametri basati sulla cronologia recente (fino a 14 giorni) oppure utilizzando la pagina Reputation metrics (Parametri di reputazione) per i parametri basati sulla cronologia complessiva fino al momento attuale.

Visualizzazione delle e-mail inviate e quota di invio utilizzata

1. Accedi alla AWS Management Console e apri la console Amazon SES all'indirizzo https://console.aws.amazon.com/ses/.
2. Nel pannello di navigazione, scegli Account dashboard (Pannello di controllo account). Le tue statistiche di utilizzo sono visualizzate nella sezione Daily email usage (Utilizzo giornaliero di e-mail).

Visualizzazione di numero di invii, percentuali di rifiuto, mancati recapiti e reclami

1. Nel pannello di navigazione, scegli Account dashboard (Pannello di controllo account).
2. Nella sezione Sending statistics (Statistiche di invio), usa il menu a discesa Date range (Intervallo date) per selezionare un valore iniziale per un intervallo di date in modo da filtrare i quattro grafici direttamente sotto la sezione Sending statistics (Statistiche di invio).
3. In base all'intervallo di date selezionato, puoi visualizzare quali erano i numeri e le percentuali in passato con la progressione dei cambiamenti del parametro fino ad oggi.
4. In uno di questi grafici, scegli il pulsante View in CloudWatch (Visualizza in CloudWatch) per aprire il rispettivo parametro nella console Amazon CloudWatch in cui puoi visualizzare dati dettagliati, eseguire calcoli personalizzati dei parametri e creare allarmi per il monitoraggio in CloudWatch.

Visualizzazione delle percentuali di mancati recapiti e reclami

1. Nel pannello di navigazione scegli Parametri di reputazione.

2. Nel pannello Percentuale di mancati recapiti puoi visualizzare la percentuale di e-mail inviate dal tuo account che hanno generato un mancato recapito permanente e nel pannello Percentuale di reclami è possibile visualizzare la percentuale di e-mail inviate dal tuo account che i destinatari hanno segnalato come spam; entrambi i parametri sono calcolati su un volume rappresentativo di e-mail in base alle procedure di invio tipiche.
3. In uno di questi grafici, scegli il pulsante Visualizza in CloudWatch per aprire il rispettivo parametro nella console Amazon CloudWatch in cui puoi visualizzare dati dettagliati, eseguire calcoli personalizzati dei parametri e creare allarmi per il monitoraggio in CloudWatch.

Visualizzazione dei parametri di reputazione per set di configurazione

1. Nel pannello di navigazione scegli Parametri di reputazione.
2. Nella pagina Parametri di reputazione, selezionare la scheda Set di configurazione.
3. Nel pannello Reputazione per set di configurazione, fai clic all'interno delcampo Set di configurazione e inizia a digitare o selezionare un set di configurazione con le metriche di reputazione abilitate.
4. Dopo aver selezionato il set di configurazione, caricherà i riquadri Riepilogo, Mancato recapito e Reclami che mostrano i parametri basati solo sull'e-mail inviata con il set di configurazione selezionato.

Monitoraggio delle statistiche di utilizzo tramite l'API Amazon SES

L'API Amazon SES fornisce l'operazione `GetSendStatistics`, che restituisce informazioni sull'utilizzo del servizio. Ti consigliamo di controllare regolarmente le statistiche di invio, per poter apportare le necessarie modifiche.

Quando chiami l'operazione `GetSendStatistics`, ricevi un elenco di punti dati che rappresentano le ultime due settimane dell'attività di invio. Ogni punto dati in questo elenco rappresenta 15 minuti di attività e contiene le informazioni indicate di seguito per tale periodo:

- numero di mancati recapiti permanenti;
- numero di reclami;
- numero di tentativi di consegna (corrispondente al numero di e-mail che hai inviato);
- numero di tentativi di invio rifiutati;
- timestamp per il periodo di analisi.

Per una descrizione completa dell'operazione `GetSendStatistics`, vedere la Documentazione di riferimento per le API di Amazon Simple Email.

In questa sezione vengono trattati gli argomenti seguenti:

Chiamata dell'operazione API **`GetSendStatistics`** tramite AWS CLI

Il modo più semplice per chiamare l'operazione API `GetSendStatistics` consiste nell'usare AWS Command Line Interface (AWS CLI).

Chiamata dell'operazione API **`GetSendStatistics`** tramite AWS CLI

1. Se non lo hai già fatto, installa l'AWS CLI. Per ulteriori informazioni, consulta la pagina relativa alla "Installazione dell'AWS Command Line Interface" nella Guida per l'utente di AWS Command Line Interface.
2. Se non lo hai già fatto, configura l'AWS CLI per l'uso delle tue credenziali AWS. Per ulteriori informazioni, consulta "Configurazione dell'AWS CLI" nella Guida per l'utente di AWS Command Line Interface.
3. Alla riga di comando esegui il comando riportato di seguito:

   ```
   aws ses get-send-statistics
   ```

   Se AWS CLI è configurato correttamente, verrà visualizzato un elenco di statistiche di invio in formato JSON. Ogni oggetto JSON include le statistiche di invio aggregate per un periodo di 15 minuti.

Chiamata dell'operazione **`GetSendStatistics`** a livello di programmazione

Puoi chiamare l'operazione `GetSendStatistics` anche tramite gli SDK AWS. Questa sezione include esempi di codice per gli SDK AWS per Go, PHP, Python e Ruby. Scegli uno dei collegamenti seguenti per visualizzare gli esempi di codice per ogni linguaggio:

- Esempio di codice per AWS SDK for Go

- Esempio di codice per AWS SDK for PHP
- Esempio di codice per AWS SDK for Python (Boto)
- Esempio di codice per AWS SDK for Ruby

> **Note**
>
> Questi esempi di codice presuppongono che tu abbia creato un file delle credenziali condiviso AWS che contiene l'ID chiave di accesso AWS, la chiave di accesso segreta AWS e la tua Regione AWS preferita. Per ulteriori informazioni, consulta l'argomento relativo ai file di configurazione e delle credenziali.

Chiamata di **`GetSendStatistics`** tramite 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)
}
```

Chiamata di **`GetSendStatistics`** tramite 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");
}

?>
```

Chiamata di **GetSendStatistics** tramite 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))
```

Chiamata di **GetSendStatistics** tramite 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
```

Monitoraggio dell'invio di e-mail utilizzando la pubblicazione di eventi di Amazon SES

Per consentirti di tracciare l'invio di e-mail a livello granulare, puoi configurare Amazon SES per pubblicare eventi di invio e-mail su Amazon CloudWatch, Amazon Data Firehose, Amazon Pinpoint o Amazon Simple Notification Service in base a caratteristiche da te definite.

Puoi tenere traccia di diversi tipi di eventi di invio di e-mail, inclusi gli invii, le consegne, le aperture, i clic, i mancati recapiti, i reclami, i rifiuti, gli errori di rendering e i ritardi di consegna. Queste informazioni possono essere utili a fini operativi e analitici. Ad esempio, puoi pubblicare i dati di invio di e-mail CloudWatch e creare dashboard che tengono traccia delle prestazioni delle tue campagne e-mail oppure puoi utilizzare Amazon SNS per inviarti notifiche quando si verificano determinati eventi.

Come funziona la pubblicazione degli eventi con i set di configurazione e i tag dei messaggi

Per utilizzare la pubblicazione degli eventi, devi prima impostare uno o più set di configurazione. Un set di configurazione specifica dove pubblicare i tuoi eventi e quali pubblicare. Quindi, ogni volta che invii un'e-mail, devi fornire il nome del set di configurazione e uno o più tag di messaggio, sotto forma di coppie nome/valore, per classificare l'e-mail. Ad esempio, se pubblicizzi libri, puoi denominare un tag di messaggio genere e assegnare il valore fantascienza o western quando invii un'e-mail per la campagna associata.

A seconda dell'interfaccia di invio e-mail utilizzata, è possibile fornire il tag del messaggio come parametro al `EmailTags`campo dell'operazione `SendEmail`API o aggiungere il tag del messaggio all'intestazione dell'e-mail specifica per SES. `X-SES-MESSAGE-TAGS` Per ulteriori informazioni sui set di configurazione, consulta Utilizzo dei set di configurazione in Amazon SES.

Oltre ai tag di messaggio specificati da te, Amazon SES aggiunge tag automatici ai messaggi inviati. Non è necessario eseguire operazioni aggiuntive per utilizzare i tag automatici.

La tabella seguente elenca i tag automatici che vengono automaticamente applicati ai messaggi inviati tramite Amazon SES.

Tag automatici Amazon SES

Nome tag automatico	Descrizione
`ses:caller-identity`	L'identità IAM dell'utente di Amazon SES che ha inviato l'e-mail.
`ses:configuration-set`	Il nome del set di configurazione associato all'email.
`ses:from-domain`	Il dominio dell'indirizzo del mittente.
`ses:outgoing-ip`	L'indirizzo IP che Amazon SES ha utilizzato per inviare l'e-mail.
`ses:source-ip`	L'indirizzo IP che l'intermediario ha utilizzato per inviare l'e-mail.
`ses:source-tls-version`	La versione del protocollo TLS utilizzata dal chiamante per inviare l'e-mail.

Feedback dettagliato per le campagne e-mail

Il `ses:feedback-id-<a or b>` tag è un tag di messaggio opzionale che puoi considerare un tag ibrido o semiautomatico: sebbene sia simile ai tag automatici discussi nella sezione precedente, la differenza è che devi aggiungerlo manualmente e utilizzare la chiave prefisso. `ses:` Puoi utilizzare fino a due di questi tag, definiti come e. `ses:feedback-id-a` `ses:feedback-id-b`

Quando si specificano questi tag, SES li aggiunge automaticamente all'`Feedback-ID`intestazione standard utilizzata per fornire statistiche sulla consegna, come le percentuali di reclami e spam, nell'ambito di un ciclo di feedback (FBL), vedi. Circuiti di feedback L'`Feedback-ID`intestazione comprende l'identificatore SESInternalID, utilizzato da SES per raccogliere informazioni sui reclami, e il tag statico, AmazonSES, che identifica SES come piattaforma di invio, ad esempio:

```
FeedBackId:feedback-id-a:feedback-id-b:((SESInternalID):(AmazonSES))
```

Questi tag ID di feedback opzionali consentono di generare feedback dettagliati, ad esempio per i messaggi inviati nell'ambito di una campagna e-mail. È possibile utilizzarlo `ses:feedback-id-<a or b>` specificandolo come tag del messaggio nel `EmailTags`campo della richiesta di `SendEmail`operazione, come mostrato nell'esempio seguente:

```
{
  "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"
}
```

Se si invia in formato raw, è necessario aggiungerlo `ses:feedback-id-<a or b>` come tag del messaggio all'intestazione specifica di SES. `X-SES-MESSAGE-TAGS`

Il tag del `ses:feedback-id-<a or b>` messaggio può anche essere monitorato in Amazon CloudWatch specificandolo come fonte di CloudWatch valore proprio come qualsiasi altro tag di messaggio, vedi the section called “Aggiungere dettagli sulla destinazione dell' CloudWatch evento” (Si applicano costi aggiuntivi, vedi Prezzo per metrica per). CloudWatch

Utilizzo della pubblicazione degli eventi

Le sezioni seguenti contengono le informazioni necessarie per configurare e utilizzare la pubblicazione degli eventi Amazon SES.

- Impostazione della pubblicazione di eventi
- Utilizzo dei dati degli eventi

Terminologia relativa alla pubblicazione degli eventi

L'elenco seguente definisce i termini correlati alla pubblicazione degli eventi Amazon SES.

Evento di invio di e-mail

Informazioni associate all'esito di un invio di un'e-mail ad Amazon SES. Gli eventi di invio includono quanto segue:

- Send (Invio): la richiesta di invio è stata completata e Amazon SES tenterà la consegna del messaggio al server di posta del destinatario. Se viene utilizzata l'eliminazione globale o a livello di account, SES la conteggia comunque come invio, ma la consegna viene eliminata.
- RenderingFailure— L'e-mail non è stata inviata a causa di un problema di visualizzazione del modello. Questo tipo di evento può verificarsi se i dati del modello mancano o se non vi è corrispondenza tra i parametri e i dati del modello. Questo tipo di evento si verifica solo quando invii un'e-mail basata su modello utilizzando le operazioni API `SendTemplatedEmail` o `SendBulkTemplatedEmail`.
- Reject (Rifiuta): Amazon SES ha accettato l'e-mail, ma ha stabilito che conteneva un virus e non ha tentato di consegnarla al server di posta del destinatario.
- Delivery (Consegna): Amazon SES ha consegnato correttamente l'e-mail al server di posta del destinatario.
- Mancato recapito: un mancato recapito permanente indica che il server di posta del destinatario ha rifiutato l'e-mail in modo permanente. (I casi di soft bounce (e-mail non recapitata) sono previsti solo se Amazon SES non riesce a inviare il messaggio e-mail dopo avere ritentato per un determinato periodo di tempo).

- Complaint (Reclamo): l'e-mail è stata recapitata correttamente al server di posta del destinatario, ma il destinatario l'ha contrassegnata come spam.
- DeliveryDelay— L'e-mail non può essere recapitata al server di posta del destinatario a causa di un problema temporaneo. I ritardi di consegna possono verificarsi, ad esempio quando la casella di posta in arrivo del destinatario è piena o quando nel server di ricezione della posta elettronica si verifica un problema transitorio.
- Subscription (Sottoscrizione): l'e-mail è stata recapitata correttamente, ma il destinatario ha aggiornato le preferenze di sottoscrizione facendo clic su `List-Unsubscribe` nell'intestazione dell'email o sul collegamento `Unsubscribe` nel piè di pagina.
- Open (Apri): il destinatario ha ricevuto il messaggio e lo ha aperto nel proprio client e-mail.
- Click (Clic): il destinatario ha fatto clic su uno o più collegamenti contenuti nell'e-mail.

Set di configurazione

Un insieme di regole che definisce la destinazione in cui Amazon SES pubblica gli eventi di invio e-mail e i tipi di eventi di invio e-mail che desideri pubblicare. Quando invii un'e-mail che desideri utilizzare con la pubblicazione degli eventi, devi specificare il set di configurazione da associare all'e-mail.

Destinazione di evento

Un AWS servizio su cui pubblicare eventi di invio e-mail di Amazon SES. Ogni destinazione impostata appartiene a un solo set di configurazione.

Tag di messaggio

Una coppia nome/valore utilizzata per classificare un'e-mail a scopo di pubblicazione degli eventi. Alcuni esempi sono campagna/libro e campagna/abbigliamento. Quando invii un'e-mail, puoi specificare il tag di messaggio come parametro per la chiamata API o come intestazione e-mail specifica di Amazon SES.

Tag automatico

Tag di messaggio che vengono automaticamente inclusi nei report di pubblicazione degli eventi. È disponibile un tag automatico per il nome del set di configurazione, il dominio dell'indirizzo "Da", l'indirizzo IP in uscita del chiamante, l'indirizzo IP in uscita di Amazon SES, e l'identità IAM del chiamante.

Impostazione della pubblicazione di eventi Amazon SES

Questa sezione descrive la procedura necessaria per configurare Amazon SES in modo da pubblicare i tuoi eventi di invio di e-mail nei seguenti servizi AWS:

- Amazon CloudWatch
- Amazon Data Firehose
- Amazon Pinpoint
- Servizio di notifica semplice Amazon (Amazon Simple Notification Service (Amazon SNS))

I seguenti passaggi necessari per impostare la pubblicazione degli eventi sono trattati negli argomenti riportati di seguito:

1. Per prima cosa devi creare un set di configurazione utilizzando la console o l'API Amazon SES.
2. Aggiungi una o più destinazioni di eventi (CloudWatch, Firehose, Pinpoint o SNS) al set di configurazione e configura i parametri unici per la destinazione dell'evento.
3. Specifica un set di configurazione che contenga la destinazione dell'evento quando invii un messaggio di posta elettronica.

Argomenti in questa sezione

Fase 1: creazione di un set di configurazione

È innanzitutto necessario disporre di un set di configurazione per impostare la pubblicazione degli eventi. Se non disponi ancora di un set di configurazione o desideri crearne uno nuovo, consulta Creazione di set di configurazione in SES

È inoltre possibile creare set di configurazione utilizzando l'operazione CreateConfigurationSet nell'API V2 Amazon SES o la CLI v2 di Amazon SES; consulta Creazione di un set di configurazione (AWS CLI).

Fase 2: aggiunta di una destinazione degli eventi

Le destinazioni degli eventi sono le posizioni in cui Amazon SES pubblica gli eventi. Ogni destinazione impostata appartiene a un solo set di configurazione. Quando configuri la destinazione di un evento con Amazon SES, scegli la destinazione del AWS servizio e specifichi i parametri associati a tale destinazione.

Quando configuri la destinazione di un evento, puoi scegliere di inviare eventi a uno dei seguenti AWS servizi:

- Amazon CloudWatch
- Amazon Data Firehose
- Amazon EventBridge
- Amazon Pinpoint
- Servizio di notifica semplice Amazon (Amazon Simple Notification Service (Amazon SNS))

La destinazione che scegli dipende dal livello di dettaglio che desideri per gli eventi e dal modo in cui desideri ricevere le informazioni sugli eventi. Se desideri semplicemente un totale progressivo di ogni tipo di evento (ad esempio, in modo da poter impostare un allarme quando il totale diventa troppo alto), puoi usare CloudWatch.

Se desideri registrare eventi dettagliati da inviare a un altro servizio come Amazon OpenSearch Service o Amazon Redshift per l'analisi, puoi utilizzare Firehose.

Se vuoi ricevere notifiche quando si verificano determinati eventi, puoi utilizzare Amazon SNS.

Questa sezione contiene gli argomenti seguenti.

- Imposta una CloudWatch destinazione per la pubblicazione degli eventi
- Configurare una destinazione di eventi Data Firehose per la pubblicazione di eventi Amazon SES
- Configura una EventBridge destinazione Amazon per la pubblicazione di eventi
- Configurazione di una destinazione degli eventi Amazon Pinpoint per la pubblicazione di eventi
- Configurazione di una destinazione degli eventi Amazon SNS per la pubblicazione di eventi

Imposta una CloudWatch destinazione per la pubblicazione degli eventi

Con Amazon CloudWatch Metrics, puoi utilizzare le destinazioni degli eventi per pubblicare e-mail di invio di eventi di Amazon SES. CloudWatch Poiché la destinazione di un CloudWatch evento può

essere impostata solo in un set di configurazione, devi prima creare un set di configurazione e quindi aggiungere la destinazione dell'evento al set di configurazione.

Quando aggiungete una destinazione di CloudWatch eventi a un set di configurazione, dovete scegliere una o più CloudWatch dimensioni che corrispondano ai tag dei messaggi che utilizzate quando inviate le vostre e-mail. Come i tag dei messaggi, una CloudWatch dimensione è una coppia nome/valore che consente di identificare in modo univoco una metrica.

Ad esempio, puoi disporre di tag di messaggio e di una dimensione denominata `campaign` che utilizzi per identificare la tua campagna e-mail. Quando pubblicate gli eventi di invio e-mail su CloudWatch, la scelta dei tag e delle dimensioni dei messaggi è importante perché queste scelte influiscono sulla CloudWatch fatturazione e determinano come filtrare i dati degli eventi di invio e-mail. CloudWatch

Questa sezione fornisce informazioni per aiutarvi a scegliere le dimensioni e quindi mostra come aggiungere una destinazione per CloudWatch eventi a un set di configurazione.

Argomenti in questa sezione

- Aggiunta di una destinazione degli eventi CloudWatch
- Scelta CloudWatch delle dimensioni

Aggiunta di una destinazione degli eventi CloudWatch

La procedura in questa sezione mostra come aggiungere i dettagli della destinazione CloudWatch dell'evento a un set di configurazione e presuppone che tu abbia completato i passaggi da 1 a 6 in Creazione di una destinazione degli eventi poi.

Puoi anche utilizzare l'operazione di UpdateConfigurationSetEventdestinazione nell'API Amazon SES V2 per creare e modificare le destinazioni degli eventi.

Per aggiungere i dettagli della destinazione CloudWatch dell'evento a un set di configurazione utilizzando la console

1. Queste sono le istruzioni dettagliate per la selezione CloudWatch del tipo di destinazione dell'evento nel passaggio 7 e presuppongono che tu abbia completato tutti i passaggi precedenti. Creazione di una destinazione degli eventi Dopo aver selezionato il tipo di CloudWatch destinazione, inserito un nome di destinazione e abilitato la pubblicazione degli eventi, viene visualizzato il riquadro delle CloudWatch dimensioni di Amazon, i cui campi vengono risolti nei passaggi seguenti. (Si applicano costi aggiuntivi, consulta Prezzo per metrica per.) CloudWatch

2. Per Value Source, specifica in che modo Amazon SES otterrà i dati a cui vengono trasferiti CloudWatch. Sono disponibili le seguenti sorgenti valore:

   - Message Tag (Tag di messaggio): Amazon SES recupera il nome della dimensione e il valore da un tag di messaggio che specifichi mediante un'intestazione `X-SES-MESSAGE-TAGS` o un parametro per l'API `EmailTags`. Per ulteriori informazioni sull'utilizzo dei tag di messaggio, consulta the section called “Fase 3: specificazione di un set di configurazione quando si esegue un invio”.

     > **Note**
     >
     > I tag di messaggio possono includere numeri da 0 a 9, lettere da A a Z (maiuscole e minuscole), trattini (-) e trattini di sottolineatura (_).

     Puoi inoltre utilizzare la sorgente valore Message Tag (Tag messaggio) per creare delle dimensioni in base ai tag automatici di Amazon SES. Per usare un tag automatico, digita il nome completo del tag automatico come Dimension Name (Nome dimensione). Ad esempio, per creare una dimensione in base al set di configurazione dei tag automatici, utilizza `ses:configuration-set` per Dimension Name (Nome dimensione) e il nome del set di configurazione per Default Value (Valore predefinito). Per un elenco completo dei tag automatici, consulta Come funziona la pubblicazione degli eventi con i set di configurazione e i tag dei messaggi.

   - Email Header (Intestazione e-mail): Amazon SES recupera il nome della dimensione e il valore da un'intestazione e-mail.

     > **Note**
     >
     > Non puoi usare nessuna delle seguenti intestazioni e-mail come Dimension Name (Nome della dimensione): `Received`, `To`, `From`, `DKIM-Signature`, `CC`, `message-id` o `Return-Path`.

   - Link Tag (Tag di collegamento): Amazon SES recupera il nome della dimensione e il valore da un tag che hai specificato in un collegamento. Per ulteriori informazioni sull'aggiunta di tag ai collegamenti, consulta Posso aggiungere tag ai collegamenti con identificatori univoci?.

3. Per Dimension Name, digita il nome della dimensione a cui vuoi passare CloudWatch.

> **Note**
>
> I nomi delle dimensioni possono contenere solo lettere ASCII (a-z, A-Z), numeri (0-9), caratteri di sottolineatura (_) o trattini (-). Spazi, caratteri accentati, caratteri non latini e altri caratteri speciali non sono consentiti.

4. In Default Value (Valore predefinito), digita il valore della dimensione.

> **Note**
>
> I valori delle dimensioni possono contenere solo lettere ASCII (a-z, A-Z), numeri (0-9), caratteri di sottolineatura (_), trattini (-), segni (@) e punti (.). Spazi, caratteri accentati, caratteri non latini e altri caratteri speciali non sono consentiti.

5. Se desideri aggiungere ulteriori dimensioni, scegli Add Dimension (Aggiungi dimensione). Altrimenti, scegli Next (Successivo).
6. Nella schermata di revisione, se sei soddisfatto della definizione della destinazione dell'evento, scegli Add destination (Aggiungi destinazione).

Scelta CloudWatch delle dimensioni

Quando scegli nomi e valori da utilizzare come CloudWatch dimensioni, considera i seguenti fattori:

- Prezzo per metrica: puoi visualizzare gratuitamente i parametri di base di Amazon SES. CloudWatch Tuttavia, quando raccogli i parametri utilizzando la pubblicazione di eventi, devi sostenere costi di monitoraggio CloudWatch dettagliato. Ogni combinazione univoca di tipo di evento, nome della dimensione e valore della dimensione crea una metrica diversa in. CloudWatch Quando utilizzi CloudWatch Detailed Monitoring, ti viene addebitato un costo per ogni metrica. Per questo motivo, potresti voler evitare di scegliere le dimensioni che possono sfruttare diversi valori. Ad esempio, a meno che tu non sia molto interessato a monitorare i tuoi eventi di invio di e-mail dal dominio "Da", potresti non voler definire una dimensione per il tag automatico Amazon SES `ses:from-domain` perché può richiedere molti valori differenti. Per ulteriori informazioni, consulta la sezione Prezzi di CloudWatch.
- Filtraggio metrico: se una metrica ha più dimensioni, non è possibile accedere alla metrica in CloudWatch base a ciascuna dimensione separatamente. Per questo motivo, rifletti attentamente prima di aggiungere più di una dimensione a una singola destinazione dell'evento. CloudWatch Ad

esempio, se desideri parametri per ogni `campaign`, per una combinazione di `campaign` e `genre` hai bisogno di aggiungere due destinazioni di evento: una con solo `campaign` come dimensione e una con `campaign` e `genre` come dimensioni.

- Sorgente del valore della dimensione: in alternativa per specificare i valori della dimensione usando intestazioni specifiche di Amazon SES o il parametro all'API, puoi anche optare per Amazon SES per prendere i valori della dimensione dalle tue intestazioni nel messaggio MIME. Potresti utilizzare questa opzione se stai già utilizzando intestazioni personalizzate e non desideri modificare le tue e-mail o le chiamate dell'API di invio di e-mail per raccogliere i parametri in base ai tuoi valori dell'intestazione. Se utilizzi le tue intestazioni nel messaggio MIME per la pubblicazione di eventi Amazon SES, i nomi e i valori che utilizzi per la pubblicazione di eventi Amazon SES potrebbe includere solo lettere dalla A alla Z, numeri da 0 a 9, trattini bassi (_), chiocciole (@), trattini (-) e punti (.). Se specifichi un nome o un valore che contiene altri caratteri, la chiamata di invio e-mail avrà comunque esito positivo, ma le metriche dell'evento non verranno inviate ad Amazon CloudWatch.

Per ulteriori informazioni sui CloudWatch concetti, consulta Amazon CloudWatch Concepts nella Amazon CloudWatch User Guide.

Configurare una destinazione di eventi Data Firehose per la pubblicazione di eventi Amazon SES

Una destinazione di eventi Amazon Data Firehose rappresenta un'entità che pubblica eventi specifici di invio e-mail di Amazon SES a Firehose. Poiché una destinazione di eventi Firehose può essere impostata solo in un set di configurazione, è necessario prima creare un set di configurazione. Successivamente, aggiungi la destinazione dell'evento al set di configurazione.

La procedura in questa sezione mostra come aggiungere i dettagli della destinazione degli eventi Firehose a un set di configurazione e presuppone che siano stati completati i passaggi da 1 a 6. Creazione di una destinazione degli eventi

Puoi anche utilizzare l'operazione UpdateConfigurationSetEventDestination nella destinazione Amazon SES API V2 per creare e aggiornare le destinazioni degli eventi.

Per aggiungere i dettagli della destinazione degli eventi Firehose a un set di configurazione utilizzando la console

1. Queste sono le istruzioni dettagliate per selezionare Firehose come tipo di destinazione dell'evento nella Fase 7 e presuppongono che abbiate completato tutti i passaggi precedenti. Creazione di una destinazione degli eventi Dopo aver selezionato il tipo di destinazione Firehose,

inserito un nome di destinazione e abilitato la pubblicazione degli eventi, viene visualizzato il riquadro del flusso di distribuzione di Amazon Data Firehose, i cui campi vengono risolti nei passaggi seguenti.

2. Per Delivery stream, scegli un flusso di distribuzione Firehose esistente oppure scegli Crea nuovo stream per crearne uno nuovo utilizzando la console Firehose.

   Per informazioni sulla creazione di uno stream utilizzando la console Firehose, consulta Creating an Amazon Kinesis Firehose Delivery Stream nella Amazon Data Firehose Developer Guide.

3. Per il ruolo Identity and Access Management (IAM), scegli un ruolo IAM per il quale Amazon SES è autorizzato a pubblicare su Firehose per tuo conto. Puoi scegliere un ruolo esistente, far sì che Amazon SES crei un ruolo per te oppure creare il tuo ruolo.

   Se scegli un ruolo esistente o crei il tuo ruolo, devi modificare manualmente le politiche del ruolo per autorizzarlo ad accedere al flusso di distribuzione di Firehose e autorizzare Amazon SES ad assumere il ruolo. Per esempi di policy, consulta Autorizzazione alla pubblicazione su Firehose Delivery Stream di Amazon SES.

4. Seleziona Next (Successivo).

5. Nella schermata di revisione, se sei soddisfatto della definizione della destinazione dell'evento, scegli Add destination (Aggiungi destinazione).

Per informazioni su come utilizzare l'`UpdateConfigurationSetEventDestination`API per aggiungere una destinazione di eventi Firehose, consulta Amazon Simple Email Service API Reference.

Autorizzazione alla pubblicazione su Firehose Delivery Stream di Amazon SES

Per consentire ad Amazon SES di pubblicare record nel tuo flusso di distribuzione Firehose, devi utilizzare un ruolo AWS Identity and Access Management (IAM) e allegare o modificare la politica di autorizzazione e la politica di fiducia del ruolo. La politica di autorizzazione consente al ruolo di pubblicare record nel flusso di distribuzione di Firehose e la politica di attendibilità consente ad Amazon SES di assumere il ruolo.

In questa sezione vengono forniti esempi di entrambe le policy. Per informazioni sul collegamento di policy ai ruoli IAM, consulta la pagina relativa alla modifica di un ruolo nella Guida per l'utente su IAM.

Policy di autorizzazione

La seguente politica di autorizzazioni consente al ruolo di pubblicare record di dati nel flusso di distribuzione di Firehose.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Action": [
        "firehose:PutRecordBatch"
      ],
      "Resource": [
        "arn:aws:firehose:delivery-region:111122223333:deliverystream/delivery-stream-name"
      ]
    }
  ]
}
```

Nel precedente esempio di policy, apporta le modifiche seguenti:

- Sostituisci *delivery-region con la AWS regione* in cui hai creato il flusso di distribuzione Firehose.
- Sostituisci *111122223333* con l'ID del tuo account AWS .
- Sostituisci *delivery-stream-name con il nome del* flusso di distribuzione Firehose.

Policy di attendibilità

La policy di attendibilità seguente consente ad Amazon SES di assumere il ruolo.

```
{
  "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"
        }
      }
    }
  ]
}
```

Nel precedente esempio di policy, apporta le modifiche seguenti:

- Sostituisci *delivery-region con la AWS regione* in cui hai creato il flusso di distribuzione Firehose.
- Sostituisci *111122223333* con l'ID del tuo account AWS .
- Sostituite *configuration-set-name con il nome* del set di configurazione associato al flusso di distribuzione di Firehose.

Configura una EventBridge destinazione Amazon per la pubblicazione di eventi

Una destinazione di EventBridge eventi Amazon ti notifica gli eventi di invio di e-mail specificati in un set di configurazione. SES genera e invia eventi di invio di e-mail al bus di eventi EventBridge predefinito. Un bus di eventi è un router che riceve eventi e può inviarli a più destinazioni. Puoi trovare ulteriori informazioni sull'integrazione degli eventi di invio di e-mail con Amazon EventBridge inMonitoraggio tramite EventBridge. Poiché la destinazione di un EventBridge evento può essere impostata solo in un set di configurazione, è necessario creare un set di configurazione prima di aggiungere la destinazione dell'evento al set di configurazione.

La procedura in questa sezione mostra come aggiungere i dettagli della destinazione EventBridge dell'evento a un set di configurazione e presuppone che siano stati completati i passaggi da 1 a 6 in Creazione di una destinazione degli eventi poi.

Puoi anche utilizzare l'operazione di UpdateConfigurationSetEventdestinazione nell'API Amazon SES V2 per creare e modificare le destinazioni degli eventi.

Per aggiungere i dettagli della destinazione EventBridge dell'evento a un set di configurazione utilizzando la console

1. Queste sono le istruzioni dettagliate per la selezione EventBridge del tipo di destinazione dell'evento nel passaggio 7 e presuppongono che tu abbia completato tutti i passaggi precedenti. Creazione di una destinazione degli eventi Dopo aver selezionato il tipo di EventBridge destinazione Amazon, inserito un nome di destinazione e abilitato la pubblicazione degli eventi, viene visualizzato il riquadro informativo Amazon EventBridge Event Bus.
2. Seleziona Next (Successivo).
3. Nella schermata di revisione, se sei soddisfatto della definizione della destinazione dell'evento, scegli Add destination (Aggiungi destinazione). In questo modo verrà aperta la pagina di riepilogo della destinazione dell'evento, in cui un banner di esito positivo confermerà se la destinazione dell'evento è stata creata o modificata correttamente.

Configurazione di una destinazione degli eventi Amazon Pinpoint per la pubblicazione di eventi

Una destinazione di eventi Amazon Pinpoint ti avvisa degli eventi di invio e-mail specificati in un set di configurazione. Poiché una destinazione di eventi Amazon Pinpoint può essere configurata solo in un set di configurazione, è necessario creare un set di configurazione prima di aggiungere la destinazione dell'evento al set di configurazione.

La procedura in questa sezione mostra come aggiungere i dettagli di una destinazione di eventi Amazon Pinpoint a un set di configurazione e considera che tu abbia completato le fasi da 1 a 6 in Creazione di una destinazione degli eventi.

Puoi anche utilizzare l'operazione di UpdateConfigurationSetEventdestinazione nell'API Amazon SES V2 per creare e modificare le destinazioni degli eventi.

Sono previsti costi aggiuntivi per i tipi di canali che hai configurato nei tuoi progetti Amazon Pinpoint. Per ulteriori informazioni, consulta Prezzi di Amazon Pinpoint.

Aggiunta di dettagli per una destinazione di eventi Amazon Pinpoint a un set di configurazione utilizzando la console

1. Queste sono le istruzioni dettagliate per selezionare Amazon Pinpoint come tipo di destinazione dell'evento in Fase 7 e presuppone di aver completato tutti i passaggi precedenti in Creazione di una destinazione degli eventi.

> **Note**
>
> Amazon Pinpoint non supporta i tipi di evento Delivery delays (Ritardi di consegna) o Subscriptions (Sottoscrizioni).

Dopo aver selezionato il tipo di destinazione Amazon Pinpoint, inserito un nome di destinazione e abilitato la pubblicazione degli eventi, viene visualizzato il riquadro dei dettagli del progetto Amazon Pinpoint, i cui campi vengono risolti nei passaggi seguenti.

2. Per Project (Progetto), scegli un progetto Amazon Pinpoint esistente oppure Create a new project in Amazon Pinpoint (Crea un nuovo progetto in Amazon Pinpoint) per crearne uno nuovo.

   Per informazioni su come creare un progetto, vedi Creazione di un progetto nella Guida per l'utente di Amazon Pinpoint.

3. Seleziona Next (Successivo).

4. Nella schermata di revisione, se sei soddisfatto della definizione della destinazione dell'evento, scegli Add destination (Aggiungi destinazione). In questo modo verrà aperta la pagina di riepilogo della destinazione dell'evento, in cui un banner di esito positivo confermerà se la destinazione dell'evento è stata creata o modificata correttamente.

Configurazione di una destinazione degli eventi Amazon SNS per la pubblicazione di eventi

Una destinazione di eventi Amazon SNS ti notifica gli eventi di invio e-mail specificati in un set di configurazione. Poiché una destinazione di eventi Amazon SNS può essere configurata solo in un set di configurazione, è necessario creare un set di configurazione prima di aggiungere la destinazione dell'evento al set di configurazione.

La procedura in questa sezione mostra come aggiungere i dettagli di una destinazione di eventi Amazon SNS a un set di configurazione e considera che tu abbia completato le fasi da 1 a 6 in Creazione di una destinazione degli eventi.

Puoi anche utilizzare l'operazione di UpdateConfigurationSetEventdestinazione nell'API Amazon SES V2 per creare e modificare le destinazioni degli eventi.

> **Note**
>
> È possibile utilizzare anche Amazon SNS per impostare le notifiche dei feedback per mancati recapiti, reclami e recapiti per qualsiasi identità di invio verificata. Per ulteriori informazioni, consulta the section called “Configurazione delle notifiche Amazon SNS”.

Sono previsti costi aggiuntivi per l'invio di messaggi agli endpoint sottoscritti ai tuoi argomenti Amazon SNS. Per ulteriori informazioni, consulta Prezzi di Amazon SNS.

Aggiunta di dettagli per una destinazione di eventi Amazon SNS a un set di configurazione utilizzando la console

1. Queste sono le istruzioni dettagliate per selezionare Amazon SNS come tipo di destinazione dell'evento in Fase 7 e presuppone di aver completato tutti i passaggi precedenti in Creazione di una destinazione degli eventi. Dopo aver selezionato il tipo di destinazione Amazon SNS, inserito un nome di destinazione e abilitato la pubblicazione degli eventi, viene visualizzato il riquadro degli argomenti Amazon Simple Notification Service (SNS), i cui campi vengono risolti nei passaggi seguenti.
2. Per SNS topic (Argomento SNS) scegli un argomento Amazon SNS esistente oppure Create SNS topic (Crea argomento SNS) per crearne uno nuovo.

   Per informazioni su come creare un argomento, consulta Creazione di un argomento nella Guida per gli sviluppatori di Amazon Simple Notification Service.

   > **Important**
   >
   > Quando crei il tuo argomento utilizzando Amazon SNS, per Type (Tipo), scegli solo Standard. (SES non supporta argomenti di tipo FIFO).

3. Seleziona Next (Successivo).
4. Nella schermata di revisione, se sei soddisfatto della definizione della destinazione dell'evento, scegli Add destination (Aggiungi destinazione). In questo modo verrà aperta la pagina di riepilogo della destinazione dell'evento, in cui un banner di esito positivo confermerà se la destinazione dell'evento è stata creata o modificata correttamente.
5. Sia che tu abbia creato un nuovo argomento SNS o ne abbia selezionato uno esistente, ora dovrai concedere l'accesso a SES per pubblicare le notifiche sull'argomento. Nella pagina di

riepilogo della destinazione dell'evento della fase precedente, scegli Amazon SNS dalla colonna Destination type (Tipo di destinazione): questo ti porterà all'elenco Topics (Argomenti) nella console Amazon Simple Notification Service. Effettua i passaggi seguenti dalla console Amazon SNS:

a. Seleziona il nome dell'argomento SNS che hai creato o modificato nella fase precedente.

b. Nella schermata dei dettagli dell'argomento, scegli Edit (Modifica).

c. Per concedere a SES l'autorizzazione a pubblicare notifiche nell'argomento, nella schermata Edit topic (Modifica argomento) della console SNS, espandi Access policy (Policy di accesso) e in JSON editor (Editor JSON) aggiungi la policy di autorizzazione seguente:

```
{
  "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"
        }
      }
    }
  ]
}
```

Nel precedente esempio di policy, apporta le modifiche seguenti:

- Sostituisci *topic_region* con la regione AWS in cui hai creato l'argomento SNS.
- *Sostituisci 111122223333 con l'ID del tuo account.* AWS
- Sostituisci *topic_name* con il nome del tuo argomento SNS.

- Sostituisci *configuration-set-name* con il nome del set di configurazione associato alla destinazione dell'evento SNS.

d. Scegli Save changes (Salva modifiche).

Fase 3: specificazione di un set di configurazione per l'invio di un messaggio di posta elettronica

Dopo aver creato un set di configurazione e aver aggiunto una destinazione degli eventi, l'ultima fase della pubblicazione di eventi consiste nell'inviare le tue e-mail.

Per pubblicare gli eventi associati a un'e-mail, devi fornire il nome del set di configurazione da associare all'e-mail. Opzionalmente puoi fornire tag di messaggio per classificare l'e-mail.

Puoi fornire queste informazioni ad Amazon SES come parametri dell'API di invio di e-mail, intestazioni specifiche di Amazon SES o intestazioni personalizzate nel messaggio MIME. Il metodo scelto dipende da quale interfaccia di invio di e-mail utilizzi, come illustrato nella seguente tabella.

Interfaccia di invio di e-mail	Metodi di pubblicazione di eventi
`SendEmail`	Parametri dell'API
`SendTemplatedEmail`	Parametri dell'API
`SendBulkTtemplatedEmail`	Parametri dell'API
`SendCustomVerificationEmail`	Parametri dell'API
`SendRawEmail`	Parametri dell'API, intestazioni e-mail specifiche di Amazon SES o intestazioni MIME personalizzate **Important** Se specifichi tag di messaggio utilizzando sia le intestazioni che i parametri dell'API, Amazon SES utilizza solo i tag di messaggio forniti dai parametri dell'API. Amazon SES non unisce i tag

Interfaccia di invio di e-mail	Metodi di pubblicazione di eventi
	di messaggio specificati dai parametri dell'API e dalle intestazioni.
Interfaccia SMTP	Intestazioni e-mail specifiche di Amazon SES

Le sezioni seguenti descrivono come specificare il set di configurazione e i tag di messaggio utilizzando le intestazioni e i parametri dell'API.

- Utilizzo di parametri dell'API Amazon SES
- Utilizzo di intestazioni e-mail specifiche di Amazon SES
- Utilizzo di intestazioni e-mail personalizzate

> **Note**
>
> Opzionalmente puoi includere tag di messaggio nelle intestazioni dell'e-mail. I tag di messaggio possono includere numeri da 0 a 9, lettere da A a Z (maiuscole e minuscole), trattini (-) e trattini di sottolineatura (_).

Utilizzo di parametri dell'API Amazon SES

Per utilizzare SendEmail, SendTemplatedEmail, SendBulkTemplatedEmail, SendCustomVerificationEmail o SendRawEmail con la pubblicazione degli eventi, devi specificare il set di configurazione e i tag dei messaggi passando le strutture di dati denominate ConfigurationSet e MessageTag alla chiamata API.

Per ulteriori informazioni sull'uso dell'API Amazon SES, consulta Documenti di riferimento per le API di Amazon Simple Email Service.

Utilizzo di intestazioni e-mail specifiche di Amazon SES

Quando usi `SendRawEmail` o l'interfaccia SMTP, puoi specificare il set di configurazione e i tag di messaggio aggiungendo intestazioni specifiche di Amazon SES all'e-mail. Amazon SES rimuove le intestazioni prima di inviare l'e-mail. La tabella seguente mostra i nomi delle intestazioni da utilizzare.

Informazioni per la pubblicazione di eventi	Intestazione
Set di configurazione	`X-SES-CONFIGURATION-SET`
Tag di messaggio	`X-SES-MESSAGE-TAGS`

L'esempio seguente mostra il possibile aspetto delle intestazioni in un'e-mail in formato RAW inviata ad 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--
```

Utilizzo di intestazioni e-mail personalizzate

Anche se devi specificare il nome del set di configurazione utilizzando l'intestazione specifica di Amazon SES `X-SES-CONFIGURATION-SET`, puoi specificare i tag di messaggio utilizzando le tue intestazioni MIME.

> **Note**
>
> I nomi e i valori delle intestazioni che usi per la pubblicazione di eventi Amazon SES devono essere in ASCII. Se specifichi un nome o un valore di intestazione non ASCII per

la pubblicazione di eventi Amazon SES, la chiamata di invio di e-mail avrà comunque esito positivo, ma i parametri degli eventi non verranno emessi in Amazon CloudWatch.

Utilizzo dei dati degli eventi Amazon SES

Dopo aver configurato la pubblicazione degli eventi e specificato un set di configurazione per l'invio di e-mail, puoi recuperare gli eventi di invio di e-mail dalla destinazione degli eventi specificata quando hai impostato il set di configurazione associato all'e-mail.

Questa sezione descrive come recuperare gli eventi di invio di e-mail da Amazon CloudWatch e Amazon Data Firehose e come interpretare i dati sugli eventi forniti da Amazon SNS.

- Recupero di dati relativi a eventi di Amazon SES da CloudWatch
- Recupero dei dati degli eventi Amazon SES da Firehose
- Interpretazione dei dati di eventi Amazon SES da Amazon SNS

Recupero di dati relativi a eventi di Amazon SES da CloudWatch

Amazon SES può pubblicare parametri di eventi di invio di e-mail ad Amazon CloudWatch. Quando pubblichi i dati degli eventi in CloudWatch, i parametri vengono forniti sotto forma di set ordinato di dati di serie temporali. Puoi utilizzare questi parametri per controllare le prestazioni dell'invio di e-mail. Ad esempio, puoi monitorare il parametro dei reclami e impostare un allarme CloudWatch che si attiva quando il parametro supera un determinato valore.

Sono disponibili due livelli di granularità a cui Amazon SES può pubblicare tali eventi in CloudWatch:

- Nell'account Account AWS: queste metriche con granularità grossolana, corrispondenti alle metriche monitorate tramite la console Amazon SES e l'API `GetSendStatistics`, sono totali riferiti all'intero Account AWS. Amazon SES pubblica questi parametri in CloudWatch automaticamente.
- A livello granulare: questi parametri sono classificati in base alle caratteristiche e-mail definite utilizzando i tag di messaggio. Per pubblicare questi parametri in CloudWatch, devi configurare la pubblicazione degli eventi con una destinazione CloudWatch e specificare un set di configurazione quando invii un'e-mail. Puoi anche specificare tag di messaggio o utilizzare tag automatici forniti automaticamente da Amazon SES.

Questa sezione descrive i parametri disponibili e come visualizzarli in CloudWatch.

Parametri disponibili

Puoi pubblicare in CloudWatch i seguenti parametri Amazon SES di eventi di invio di e-mail:

- Send (Invia): la richiesta di invio è stata completata e Amazon SES tenterà la consegna del messaggio al server di posta del destinatario. Se viene utilizzata l'eliminazione globale o a livello di account, SES la conteggia comunque come invio, ma la consegna viene eliminata.
- RenderingFailure: l'e-mail non è stata inviata a causa di un errore di rendering del modello. Questo tipo di evento può verificarsi se i dati del modello mancano o se non vi è corrispondenza tra i parametri e i dati del modello. Questo tipo di evento si verifica solo quando invii un'e-mail basata su modello utilizzando le operazioni API `SendTemplatedEmail` o `SendBulkTemplatedEmail`.
- Reject (Rifiuta): Amazon SES ha accettato l'e-mail, ma ha stabilito che conteneva un virus e non ha tentato di consegnarla al server di posta del destinatario.
- Delivery (Consegna): Amazon SES ha consegnato correttamente l'e-mail al server di posta del destinatario.
- Mancato recapito: un mancato recapito permanente indica che il server di posta del destinatario ha rifiutato l'e-mail in modo permanente. (I casi di soft bounce (e-mail non recapitata) sono previsti solo se Amazon SES non riesce a inviare il messaggio e-mail dopo avere ritentato per un determinato periodo di tempo).
- Complaint (Reclamo): l'e-mail è stata recapitata correttamente al server di posta del destinatario, ma il destinatario l'ha contrassegnata come spam.
- DeliveryDelay: impossibile recapitare l'e-mail al server di posta del destinatario perché si è verificato un problema temporaneo. I ritardi di consegna possono verificarsi, ad esempio quando la casella di posta in arrivo del destinatario è piena o quando nel server di ricezione della posta elettronica si verifica un problema transitorio.
- Subscription (Sottoscrizione): l'e-mail è stata recapitata correttamente, ma il destinatario ha aggiornato le preferenze di sottoscrizione facendo clic su `List-Unsubscribe` nell'intestazione dell'email o sul collegamento `Unsubscribe` nel piè di pagina.
- Open (Apri): il destinatario ha ricevuto il messaggio e lo ha aperto nel proprio client e-mail.
- Click (Clic): il destinatario ha fatto clic su uno o più collegamenti contenuti nell'e-mail.

Dimensioni disponibili

CloudWatch usa i nomi di dimensione specificati durante l'aggiunta di una destinazione di eventi CloudWatch a un set di configurazione in Amazon SES. Per ulteriori informazioni, consulta Imposta una CloudWatch destinazione per la pubblicazione degli eventi.

Visualizzazione dei parametri Amazon SES nella console CloudWatch

La procedura seguente descrive come visualizzare i parametri Amazon SES di pubblicazione degli eventi tramite la console CloudWatch.

Visualizzazione dei parametri utilizzando la console CloudWatch

1. Accedi all'AWS Management Console e apri la console CloudWatch all'indirizzo https://console.aws.amazon.com/cloudwatch/.
2. Se necessario, modifica la regione. Nella barra di navigazione seleziona la regione in cui si trovano le risorse AWS. Per ulteriori informazioni, consulta Regioni ed endpoint di .
3. Nel riquadro di navigazione, seleziona Tutti i parametri.
4. Nel riquadro Parametri IP, seleziona SES.
5. Scegli il parametro da visualizzare. Per visualizzare i parametri di pubblicazione degli eventi a livello granulare, scegli la combinazione di dimensioni specificate al momento della configurazione della destinazione degli eventi CloudWatch. Per ulteriori informazioni sulla visualizzazione dei parametri con CloudWatch, consulta Use Amazon CloudWatch metrics (Utilizzo dei parametri di Amazon CloudWatch).

Visualizzazione dei parametri usando AWS CLI

- Al prompt dei comandi, utilizza il comando seguente:

```
aws cloudwatch list-metrics --namespace "AWS/SES"
```

Recupero dei dati degli eventi Amazon SES da Firehose

Amazon SES pubblica gli eventi di invio di e-mail a Firehose come record JSON. Firehose pubblica quindi i record nella destinazione del AWS servizio scelta al momento della configurazione del flusso di distribuzione in Firehose. Per informazioni sulla configurazione dei flussi di distribuzione Firehose, consulta Creating an Firehose Delivery Stream nella Amazon Data Firehose Developer Guide.

Argomenti in questa sezione:

Contenuto dei dati sugli eventi che Amazon SES pubblica su Firehose

Amazon SES pubblica i record degli eventi di invio di e-mail ad Amazon Data Firehose in formato JSON. Quando pubblica eventi su Firehose, Amazon SES segue ogni record JSON con un carattere di nuova riga.

È possibile trovare record di esempio per tutti questi tipi di notifica in Esempi di dati sugli eventi che Amazon SES pubblica su Firehose.

Argomenti in questa sezione

Oggetto JSON di primo livello

L'oggetto JSON di primo livello in un record degli eventi di invio di e-mail contiene i campi riportati di seguito.

Nome campo	Descrizione
`eventType`	Una stringa che descrive il tipo di evento. Valori possibili: `Bounce`, `Complaint` , `Delivery`, `Send`, `Reject`, `Open`, `Click`, `Rendering Failure`, `DeliveryDelay` o `Subscription` . Se non hai configurato la pubblicazione di eventi, questo campo è denominato `notificationType` .
`mail`	Un oggetto JSON che contiene informazioni sull'e-mail che ha generato l'evento.
`bounce`	Questo campo è presente solo se `eventType` è `Bounce`. Contiene informazioni sul mancato recapito.
`complaint`	Questo campo è presente solo se `eventType` è `Complaint` . Contiene informazioni sul reclamo.
`delivery`	Questo campo è presente solo se `eventType` è `Delivery`. Contiene informazioni sulla consegna.
`send`	Questo campo è presente solo se `eventType` è `Send`.
`reject`	Questo campo è presente solo se `eventType` è `Reject`. Contiene informazioni sul rifiuto.
`open`	Questo campo è presente solo se `eventType` è `Open`. Contiene informazioni sull'evento di apertura.

Nome campo	Descrizione
`click`	Questo campo è presente solo se `eventType` è `Click`. Contiene informazioni sull'evento clic.
`failure`	Questo campo è presente solo se `eventType` è `Rendering Failure` . Contiene informazioni sull'evento di errore di rendering.
`deliveryDelay`	Questo campo è presente solo se `eventType` è `DeliveryDelay` . Contiene informazioni sulla consegna ritardata di un'e-mail.
`subscription`	Questo campo è presente solo se `eventType` è `Subscription` . Contiene informazioni sulle preferenze relative alle sottoscrizioni.

Oggetto mail

Ogni record di eventi di invio di e-mail contiene informazioni sull'e-mail originale nell'oggetto `mail`. L'oggetto JSON che contiene informazioni su un oggetto `mail` include i campi riportati di seguito.

Nome campo	Descrizione
`timestamp`	La data e l'ora di invio del messaggio, in formato ISO8601 (AAAA-MM-GGThh:mm:ss.sZ).
`messageId`	Un ID univoco che Amazon SES ha assegnato al messaggio. Amazon SES ti ha restituito questo valore quando hai inviato il messaggio. **Note** Questo è l'ID messaggio assegnato da Amazon SES. Puoi trovare l'ID messaggio dell'e-mail originale nei

Nome campo	Descrizione
	campi `headers` e `commonHeaders` dell'oggetto `mail`.
`source`	L'indirizzo e-mail da cui il messaggio è stato inviato (indirizzo MAIL FROM della busta).
`sourceArn`	L'Amazon Resource Name (ARN) dell'identità utilizzata per inviare l'e-mail. Nel caso di autorizzazione all'invio, `sourceArn` è l'ARN dell'identità che il mittente delegato è stato autorizzato a utilizzare dal proprietario dell'identità per inviare l'e-mail. Per ulteriori informazioni sull'autorizzazione all'invio, consulta Metodi di autenticazione delle e-mail.
`sendingAccountId`	L'ID dell'account AWS utilizzato per inviare l'e-mail. Nel caso di autorizzazione all'invio, `sendingAccountId` è l'ID account del mittente delegato.
`destination`	Un elenco degli indirizzi e-mail destinatari della posta originale.
`headersTruncated`	Una stringa che specifica se le intestazioni vengono troncate nella notifica. Ciò si verifica se le intestazioni hanno dimensione superiore a 10 KB. I valori possibili sono `true` e `false`.

Nome campo	Descrizione
`headers`	Un elenco delle intestazioni originali dell'e-mail. Ogni intestazione nell'elenco include un campo `name` e un campo `value`. **Note** L'ID messaggio nel campo `headers` deriva dal messaggio originale passato ad Amazon SES. L'ID messaggio che Amazon SES ha successivamente assegnato al messaggio si trova nel campo `messageId` dell'oggetto `mail`.
`commonHeaders`	Una mappatura delle intestazioni originali, di uso frequente, dell'e-mail. **Note** Qualsiasi ID messaggio all'interno del campo `commonHeaders` è quello che Amazon SES ha successivamente assegnato al messaggio nel campo `messageId` dell'oggetto `mail`.
`tags`	Un elenco di tag associati all'e-mail.

Oggetto del mancato recapito

L'oggetto JSON che contiene informazioni su un evento `Bounce` include sempre i campi riportati di seguito.

Nome campo	Descrizione
`bounceType`	Il tipo di mancato recapito secondo Amazon SES.
`bounceSubType`	Il sottotipo di mancato recapito secondo Amazon SES.
`bouncedRecipients`	Elenco che contiene informazioni sui destinatari della posta originale che non è stata recapitata.
`timestamp`	La data e l'ora in cui l'ISP ha inviato la notifica di mancato recapito, in formato ISO8601 (AAAA-MM-GGThh:mm:ss.sZ).
`feedbackId`	Un ID univoco per il mancato recapito.
`reportingMTA`	Il valore del campo `Reporting-MTA` nella notifica sullo stato del recapito. Questo è il valore dell'autorità MTA (Message Transfer Authority) che ha tentato di eseguire l'operazi one di consegna, inoltro o gateway descritta nella notifica. **Note** Il campo è visualizzato solo se alla mancata consegna è allegata una notifica sullo stato del recapito (DSN).

Destinatari del mancato recapito

Un evento di mancato recapito può riguardare uno o più destinatari. Il campo `bouncedRecipients` include un elenco di oggetti, uno per ogni destinatario interessato dall'evento di mancato recapito, e conterrà sempre il campo seguente.

Nome campo	Descrizione
`emailAddress`	L'indirizzo e-mail del destinatario. Se è disponibile una notifica sullo stato di consegna, questo è il valore del campo `Final-Recipient` della notifica.

Opzionalmente, se una notifica sullo stato di consegna è allegata al mancato recapito, possono essere presenti anche i campi seguenti.

Nome campo	Descrizione
`action`	Il valore del campo `Action` nella notifica sullo stato del recapito. Indica l'operazione eseguita dall'autorità MTA interessata come risultato del tentativo di recapitare il messaggio a questo destinatario.
`status`	Il valore del campo `Status` nella notifica sullo stato del recapito. Questo è il codice di stato indipendente dal trasporto che indica lo stato di consegna del messaggio per ogni destinatario.
`diagnosticCode`	Il codice di stato emesso dall'autorità MTA interessata. Si tratta del valore del campo `Diagnostic-Code` nella notifica sullo stato di consegna. Il campo potrebbe non essere incluso in questa notifica, quindi nemmeno nell'oggetto JSON.

Tipi di mancato recapito

Ogni evento di mancato recapito rientra in uno dei tipi illustrati nella seguente tabella.

Il sistema di pubblicazione degli eventi pubblica solo hard bounce e soft bounce che non verranno più ritentati da Amazon SES. Quando ricevi dei mancati recapiti contrassegnati come `Permanent`,

devi rimuovere i corrispondenti indirizzi e-mail dalla tua mailing list; non sarai in grado di inviare loro dei messaggi in futuro. I mancati recapiti di tipo `Transient` vengono inviati quando si verificano più soft bounce per il messaggio e Amazon SES ha smesso di tentare di consegnarli nuovamente. In futuro, potresti riuscire nuovamente a inviare messaggi a un indirizzo che inizialmente ha generato un mancato recapito `Transient`.

bounceType	bounceSubType	Descrizione
`Undetermined`	`Undetermined`	Amazon SES non è stato in grado di determinare un motivo specifico per il mancato recapito.
`Permanent`	`General`	Amazon SES ha ricevuto un mancato recapito permanente generale. Se ricevi questo tipo di mancato recapito, devi eliminare l'indirizzo e-mail del destinatario dalla lista di distribuzione.
`Permanent`	`NoEmail`	Amazon SES ha ricevuto un mancato recapito permanente perché l'indirizzo e-mail di destinazione non esiste. Se ricevi questo tipo di mancato recapito, devi eliminare l'indirizzo e-mail del destinatario dalla lista di distribuzione.
`Permanent`	`Suppressed`	Amazon SES non invia più a questo indirizzo perché ha una storia recente di mancati recapiti come indirizzo non valido. Per sovrascrivere l'elenco di eliminazione globale, consulta Utilizzo dell'elenco di eliminazione a livello di account di Amazon SES.
`Permanent`	`OnAccountSuppressionList`	Amazon SES ha soppresso l'invio a questo indirizzo perché si trova nell'elenco di eliminazione a livello di account. Ciò non influisce sulla metrica relativa alla frequenza dei mancati recapiti.
`Transient`	`General`	Amazon SES ha ricevuto un mancato recapito generale. È possibile che riesca a inviare messaggi a questo destinatario in futuro.

bounceType	bounceSubType	Descrizione
`Transient`	`MailboxFull`	Amazon SES ha ricevuto un mancato recapito per casella di posta piena. È possibile che riesca a inviare messaggi a questo destinatario in futuro.
`Transient`	`MessageTooLarge`	Amazon SES ha ricevuto un mancato recapito per messaggio troppo grande. Potresti riuscire a inviare il messaggio al destinatario riducendo le dimensioni.
`Transient`	`ContentRejected`	Amazon SES ha ricevuto un mancato recapito per contenuti rifiutati. Potresti riuscire a inviare il messaggio al destinatario modificandone il contenuto.
`Transient`	`AttachmentRejected`	Amazon SES ha ricevuto un mancato recapito per allegato rifiutato. Potresti riuscire a inviare il messaggio al destinatario rimuovendo o modificando l'allegato.

Oggetto del reclamo

L'oggetto JSON che contiene informazioni su un evento `Complaint` include i campi riportati di seguito.

Nome campo	Descrizione
`complainedRecipients`	Un elenco che contiene informazioni sui destinatari che potrebbero avere inviato il reclamo.
`timestamp`	La data e l'ora in cui l'ISP ha inviato la notifica di reclamo, in formato ISO8601 (AAAA-MM-GGThh:mm:ss.sZ).
`feedbackId`	Un ID univoco per il reclamo.

Nome campo	Descrizione
`complaintSubType`	Il sottotipo del reclamo, come determinato da Amazon SES.

Inoltre, se un report di feedback è associato al reclamo, potrebbero essere presenti i campi seguenti.

Nome campo	Descrizione
`userAgent`	Il valore del campo `User-Agent` nel report di feedback. Indica il nome e la versione del sistema che ha generato il report.
`complaintFeedbackType`	Il valore del campo `Feedback-Type` nel report di feedback ricevuto dall'ISP. Contiene il tipo di feedback.
`arrivalDate`	Il valore del campo `Arrival-Date` o `Received-Date` nel report di feedback, in formato ISO8601 (AAAA-MM-GGThh:mm:ss.sZ). Il campo potrebbe non essere incluso nel report, quindi nemmeno nell'oggetto JSON.

Destinatari che hanno inviato il reclamo

Il campo `complainedRecipients` contiene un elenco di destinatari che potrebbero aver inviato il reclamo.

> **Important**
>
> Poiché la maggior parte degli ISP omette l'indirizzo e-mail del destinatario che ha inviato il reclamo dalla notifica di reclamo, questo elenco contiene informazioni sui destinatari che potrebbero aver inviato il reclamo, in base ai destinatari del messaggio originale e all'ISP da cui abbiamo ricevuto il reclamo. Amazon SES esegue una ricerca rispetto al messaggio originale per determinare l'elenco dei destinatari.

Gli oggetti JSON in questo elenco contengono il campo seguente.

Nome campo	Descrizione
`emailAddress`	L'indirizzo e-mail del destinatario.

Tipi di reclamo

Puoi visualizzare i tipi di reclamo seguenti nel campo `complaintFeedbackType`, assegnati dall'ISP che effettua la segnalazione, secondo il sito Web IANA (Internet Assigned Numbers Authority):

Nome campo	Descrizione
`abuse`	Indica un messaggio e-mail indesiderato o un altro tipo di uso illecito dell'e-mail.
`auth-failure`	Report di errore di autenticazione dell'e-mail.
`fraud`	Indica un tipo di frode o attività di phishing.
`not-spam`	Indica che l'entità che fornisce il report non considera il messaggio come spam. Può essere utilizzato per correggere un messaggio che è stato erroneamente contrassegnato o classificato come spam.
`other`	Indica qualsiasi altro feedback che non rientra in altri tipi registrati.
`virus`	Segnala la presenza di un virus nel messaggio di origine.

Oggetto di consegna

L'oggetto JSON che contiene informazioni su un evento `Delivery` include sempre i campi riportati di seguito.

Nome campo	Descrizione
`timestamp`	La data e l'ora in cui Amazon SES ha consegnato l'e-mail al server di posta del destinatario, in formato ISO8601, (AAAA-MM-GGThh:mm:ss.sZ).
`processingTimeMillis`	Il tempo in millisecondi tra quando Amazon SES ha accettato la richiesta del mittente e quando Amazon SES ha trasferito il messaggio al server di posta del destinatario.
`recipients`	Un elenco dei destinatari mirati a cui si applica l'evento di consegna.
`smtpResponse`	Il messaggio di risposta SMTP dell'ISP remoto che ha accettato l'e-mail da Amazon SES. Questo messaggio può variare in base all'e-mail, al server di posta ricevente e all'ISP ricevente.
`reportingMTA`	Il nome host del server di posta Amazon SES che ha inviato l'e-mail.

Oggetto send

L'oggetto JSON che contiene informazioni su un evento `send` è sempre vuoto.

Oggetto reject

L'oggetto JSON che contiene informazioni su un evento `Reject` include sempre i campi riportati di seguito.

Nome campo	Descrizione
`reason`	Il motivo per cui l'e-mail è stata rifiutata. L'unico valore possibile è `Bad content`, che significa che Amazon SES ha rilevato che l'e-mail

Nome campo	Descrizione
	conteneva un virus. Quando un messaggio viene rifiutato, Amazon SES ne interrompe l'elaborazione e non tenta di inviarlo al server di posta elettronica del destinatario.

Oggetto open

L'oggetto JSON che contiene informazioni su un evento `Open` include sempre i campi riportati di seguito.

Nome campo	Descrizione
`ipAddress`	L'indirizzo IP del destinatario.
`timestamp`	La data e l'ora in cui si è verificato l'evento apertura, in formato ISO8601 (AAAA-MM-GGThh:mm:ss.sZ).
`userAgent`	L'agente utente del dispositivo o del client di posta elettronica che il destinatario ha utilizzato per aprire l'e-mail.

Oggetto click

L'oggetto JSON che contiene informazioni su un evento `Click` include sempre i campi riportati di seguito.

Nome campo	Descrizione
`ipAddress`	L'indirizzo IP del destinatario.
`timestamp`	La data e l'ora in cui si è verificato l'evento clic, in formato ISO8601 (AAAA-MM-GGThh:mm:ss.sZ).

Nome campo	Descrizione
`userAgent`	L'agente utente del client che il destinatario ha utilizzato per fare clic su un collegamento nell'e-mail.
`link`	L'URL del collegamento su cui il destinatario ha fatto clic.
`linkTags`	Un elenco dei tag che sono stati aggiunti al collegamento utilizzando l'attributo `ses:tags`. Per ulteriori informazioni sull'aggiunta di tag ai collegamenti nelle e-mail, consulta D5. Posso aggiungere tag ai collegamenti con identificatori univoci? in Domande frequenti sui parametri per l'invio di e-mail con Amazon SES.

Oggetto errore di rendering

L'oggetto JSON che contiene informazioni su un evento `Rendering Failure` include i campi riportati di seguito.

Nome campo	Descrizione
`templateName`	Nome del modello usato per inviare l'e-mail.
`errorMessage`	Messaggio che fornisce altre informazioni sull'errore di rendering.

DeliveryDelay oggetto

L'oggetto JSON che contiene informazioni su un evento `DeliveryDelay` include i campi riportati di seguito.

Nome campo	Descrizione
`delayType`	Il tipo di ritardo. I valori possibili sono:

Nome campo	Descrizione
	• InternalFailure— Un problema interno di Amazon SES ha causato il ritardo del messaggio. • General: si è verificato un errore generico durante la conversazione SMTP. • MailboxFull— La casella di posta del destinatario è piena e non è in grado di ricevere messaggi aggiuntivi. • SpamDetected— Il server di posta del destinatario ha rilevato una grande quantità di e-mail indesiderate dal tuo account. • RecipientServerError— Un problema temporaneo con il server di posta elettronica del destinatario impedisce la consegna del messaggio. • IPFailure: l'indirizzo IP che invia il messaggio viene bloccato od ostacolato dal provider di posta elettronica del destinatario. • TransientCommunicationFailure— Si è verificato un errore di comunicazione temporaneo durante la conversazione SMTP con il provider di posta elettronica del destinatario. • BYOIP HostNameLookupUnavailable: Amazon SES non è riuscito a cercare il nome host DNS per i tuoi indirizzi IP. Questo tipo di ritardo si verifica solo quando si utilizza Bring Your Own IP. • Undetermined: Amazon SES non è stato in grado di determinare il motivo del ritardo di consegna.

Nome campo	Descrizione
	• SendingDeferral— Amazon SES ha ritenuto opportuno rinviare internamente il messaggio .
`delayedRecipients`	Oggetto che contiene informazioni sul destinata rio del messaggio di posta elettronica.
`expirationTime`	La data e l'ora in cui Amazon SES interrompe il tentativo di recapitare il messaggio. Questo valore è mostrato in formato ISO 8601.
`reportingMTA`	Indirizzo IP dell'agente di trasferimento messaggi (MTA) che ha segnalato il ritardo.
`timestamp`	La data e l'ora in cui si è verificato il ritardo, mostrate in formato ISO 8601.

Destinatari del ritardo di consegna

L'oggetto `delayedRecipients` include i seguenti valori.

Nome campo	Descrizione
`emailAddress`	Indirizzo di posta elettronica che ha provocato un ritardo nel recapito del messaggio.
`status`	Il codice di stato SMTP associato al ritardo di consegna.
`diagnosticCode`	Il codice diagnostico fornito dal Message Transfer Agent (MTA) ricevente.

Oggetto sottoscrizione

L'oggetto JSON che contiene informazioni su un evento `Subscription` include i campi riportati di seguito.

Nome campo	Descrizione
`contactList`	Il nome dell'elenco in cui si trova il contatto.
`timestamp`	La data e l'ora in cui l'ISP ha inviato la notifica di sottoscrizione, in formato ISO8601 (AAAA-MM-GGThh:mm:ss.sZ).
`source`	L'indirizzo e-mail da cui il messaggio è stato inviato (indirizzo MAIL FROM della busta).
`newTopicPreferences`	Una struttura dati JSON (mappa) che specifica lo stato della sottoscrizione di tutti gli argomenti dell'elenco dei contatti che indicano lo stato dopo una modifica (contatto sottoscritto o annullato).
`oldTopicPreferences`	Una struttura dati JSON (mappa) che specifica lo stato della sottoscrizione di tutti gli argomenti dell'elenco dei contatti che indicano lo stato prima della modifica (contatto sottoscritto o annullato).

Preferenze per argomento nuovo/vecchio

Gli oggetti `newTopicPreferences` e `oldTopicPreferences` includono i seguenti valori.

Nome campo	Descrizione
`unsubscribeAll`	Specifica se il contatto ha annullato la sottoscri zione a tutti gli argomenti dell'elenco dei contatti.
`topicSubscriptionStatus`	Speciifica l'argomento nel `topicName` campo e mappa lo stato dell'abbonamento (OptIno OptOut) nel campo. `subscriptionStatus`

Nome campo	Descrizione
`topicDefaultSubscriptionStatus`	Specifica l'argomento nel `topicName` campo e mappa lo stato dell'abbonamento (OptIno OptOut) nel `subscriptionStatus` campo.

Esempi di dati sugli eventi che Amazon SES pubblica su Firehose

Questa sezione fornisce esempi dei tipi di record di eventi di invio e-mail che Amazon SES pubblica su Firehose.

Argomenti in questa sezione:

- Record di eventi di mancato recapito
- Record di eventi di reclamo
- Record di eventi di consegna
- Record di eventi di invio
- Record di eventi di rifiuto
- Record di eventi di apertura
- Record di eventi di clic
- Record di eventi di errore di rendering
- DeliveryDelay record
- Registro di sottoscrizione

> **Note**
>
> Negli esempi in cui si utilizza un campo `tag`, utilizza la pubblicazione di eventi attraverso un set di configurazione per il quale SES supporta la pubblicazione di tag per tutti i tipi di evento. Se utilizzi le notifiche di feedback direttamente sull'identità, SES non pubblica tag. Ottieni ulteriori informazioni sull'aggiunta di tag durante la creazione di un set di configurazione o la modifica di un set di configurazione.

Record di eventi di mancato recapito

Di seguito è riportato un esempio di record di `Bounce` eventi che Amazon SES pubblica su 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"
      ]
    }
  }
}
```

Record di eventi di reclamo

Di seguito è riportato un esempio di record di `Complaint` eventi che Amazon SES pubblica su 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"
      ]
    }
  }
}
```

Record di eventi di consegna

Di seguito è riportato un esempio di record di `Delivery` eventi che Amazon SES pubblica su 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"
  }
}
```

Record di eventi di invio

Di seguito è riportato un esempio di record di `Send` eventi che Amazon SES pubblica su 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": {}
}
```

Record di eventi di rifiuto

Di seguito è riportato un esempio di record di `Reject` eventi che Amazon SES pubblica su 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"
  }
}
```

Record di eventi di apertura

Di seguito è riportato un esempio di record di `Open` eventi che Amazon SES pubblica su 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"
  }
```

```
}
```

Record di eventi di clic

Di seguito è riportato un esempio di record di `Click` eventi che Amazon SES pubblica su 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"
  }
}
```

Record di eventi di errore di rendering

Di seguito è riportato un esempio di record di `Rendering Failure` eventi che Amazon SES pubblica su Firehose.

```
{
  "eventType":"Rendering Failure",
  "mail":{
    "timestamp":"2018-01-22T18:43:06.197Z",
    "source":"sender@example.com",
    "sourceArn":"arn:aws:ses:us-east-1:123456789012:identity/sender@example.com",
    "sendingAccountId":"123456789012",
    "messageId":"EXAMPLE7c191be45-e9aedb9a-02f9-4d12-a87d-dd0099a07f8a-000000",
    "destination":[
      "recipient@example.com"
    ],
    "headersTruncated":false,
    "tags":{
      "ses:configuration-set":[
        "ConfigSet"
      ]
    }
  },
  "failure":{
    "errorMessage":"Attribute 'attributeName' is not present in the rendering data.",
    "templateName":"MyTemplate"
  }
}
```

DeliveryDelay record

Di seguito è riportato un esempio di record di `DeliveryDelay` eventi che Amazon SES pubblica su 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 di sottoscrizione

Di seguito è riportato un esempio di record di `Subscription` eventi che Amazon SES pubblica su 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"
        }
      ]
    }
  }
}
```

Interpretazione dei dati di eventi Amazon SES da Amazon SNS

Amazon SES pubblica gli eventi di invio di e-mail in Amazon Simple Notification Service (Amazon SNS) come record JSON. Amazon SNS, quindi, invia notifiche agli endpoint iscritti all'argomento Amazon SNS associato con la destinazione dell'evento. Per informazioni sulla creazione di un argomento Amazon SNS e sull'abbonamento allo stesso, consulta Nozioni di base su Amazon SNS nella Guida per sviluppatori di Amazon Simple Notification Service.

Per una descrizione del contenuto dei record e per record di esempio, consulta le sezioni seguenti.

- Contenuto dei record di eventi
- Esempi di record di eventi

Contenuto dei dati degli eventi pubblicati da Amazon SES su Amazon SNS

Amazon SES pubblica i record degli eventi di invio di e-mail in Amazon Simple Notification Service in formato JSON.

È possibile trovare record di esempio per tutti questi tipi di notifica in Esempi di dati degli eventi pubblicati da Amazon SES su Amazon SNS.

Argomenti in questa sezione:

Oggetto JSON di primo livello

L'oggetto JSON di primo livello in un record degli eventi di invio di e-mail contiene i campi riportati di seguito. Il tipo di evento determina quali altri oggetti sono presenti.

Nome campo	Descrizione
`eventType`	Una stringa che descrive il tipo di evento. Valori possibili: `Bounce`, `Complaint` , `Delivery`, `Send`, `Reject`, `Open`, `Click`, `Rendering Failure`, `DeliveryDelay` o `Subscription` .

Nome campo	Descrizione
	Se non hai configurato la pubblicazione di eventi, questo campo è denominato `notificationType` .
`mail`	Un oggetto JSON che contiene informazioni sull'e-mail che ha generato l'evento.
`bounce`	Questo campo è presente solo se `eventType` è `Bounce`. Contiene informazioni sul mancato recapito.
`complaint`	Questo campo è presente solo se `eventType` è `Complaint` . Contiene informazioni sul reclamo.
`delivery`	Questo campo è presente solo se `eventType` è `Delivery`. Contiene informazioni sulla consegna.
`send`	Questo campo è presente solo se `eventType` è `Send`.
`reject`	Questo campo è presente solo se `eventType` è `Reject`. Contiene informazioni sul rifiuto.
`open`	Questo campo è presente solo se `eventType` è `Open`. Contiene informazioni sull'evento di apertura.
`click`	Questo campo è presente solo se `eventType` è `Click`. Contiene informazioni sull'evento clic.
`failure`	Questo campo è presente solo se `eventType` è `Rendering Failure` . Contiene informazioni sull'evento di errore di rendering.

Nome campo	Descrizione
`deliveryDelay`	Questo campo è presente solo se `eventType` è `DeliveryDelay` . Contiene informazioni sulla consegna ritardata di un'e-mail.
`subscription`	Questo campo è presente solo se `eventType` è `Subscription` . Contiene informazioni sulle preferenze relative alle sottoscrizioni.

Oggetto mail

Ogni record di eventi di invio di e-mail contiene informazioni sull'e-mail originale nell'oggetto `mail`. L'oggetto JSON che contiene informazioni su un oggetto `mail` include i campi riportati di seguito.

Nome campo	Descrizione
`timestamp`	La data e l'ora di invio del messaggio, in formato ISO8601 (AAAA-MM-GGThh:mm:ss.sZ).
`messageId`	Un ID univoco che Amazon SES ha assegnato al messaggio. Amazon SES ti ha restituito questo valore quando hai inviato il messaggio. **Note** Questo è l'ID messaggio assegnato da Amazon SES. Puoi trovare l'ID messaggio dell'e-mail originale nei campi `headers` e `commonHeaders` dell'oggetto `mail`.
`source`	L'indirizzo e-mail da cui il messaggio è stato inviato (indirizzo MAIL FROM della busta).

Nome campo	Descrizione
`sourceArn`	L'Amazon Resource Name (ARN) dell'identità utilizzata per inviare l'e-mail. Nel caso di autorizzazione all'invio, `sourceArn` è l'ARN dell'identità che il mittente delegato è stato autorizzato a utilizzare dal proprietario dell'identità per inviare l'e-mail. Per ulteriori informazioni sull'autorizzazione all'invio, consulta Metodi di autenticazione delle e-mail.
`sendingAccountId`	L'ID dell'account AWS utilizzato per inviare l'e-mail. Nel caso di autorizzazione all'invio, `sendingAccountId` è l'ID account del mittente delegato.
`destination`	Un elenco degli indirizzi e-mail destinatari della posta originale.
`headersTruncated`	Una stringa che specifica se le intestazioni vengono troncate nella notifica. Ciò si verifica se le intestazioni hanno dimensione superiore a 10 KB. I valori possibili sono `true` e `false`.
`headers`	Un elenco delle intestazioni originali dell'e-mail. Ogni intestazione nell'elenco include un campo `name` e un campo `value`. **Note** L'ID messaggio nel campo `headers` deriva dal messaggio originale passato ad Amazon SES. L'ID messaggio che Amazon SES ha successivamente assegnato al messaggio si trova nel campo `messageId` dell'oggetto `mail`.

Nome campo	Descrizione
`commonHeaders`	Una mappatura delle intestazioni originali, di uso frequente, dell'e-mail. **Note** Qualsiasi ID messaggio all'interno del campo `commonHeaders` è quello che Amazon SES ha successivamente assegnato al messaggio nel campo `messageId` dell'oggetto `mail`.
`tags`	Un elenco di tag associati all'e-mail.

Oggetto del mancato recapito

L'oggetto JSON che contiene informazioni su un evento `Bounce` include i campi riportati di seguito.

Nome campo	Descrizione
`bounceType`	Il tipo di mancato recapito secondo Amazon SES.
`bounceSubType`	Il sottotipo di mancato recapito secondo Amazon SES.
`bouncedRecipients`	Elenco che contiene informazioni sui destinatari della posta originale che non è stata recapitata.
`timestamp`	La data e l'ora in cui l'ISP ha inviato la notifica di mancato recapito, in formato ISO8601 (AAAA-MM-GGThh:mm:ss.sZ).
`feedbackId`	Un ID univoco per il mancato recapito.
`reportingMTA`	Il valore del campo `Reporting-MTA` nella notifica sullo stato del recapito. Questo è il

Nome campo	Descrizione
	valore dell'autorità MTA (Message Transfer Authority) che ha tentato di eseguire l'operazi one di consegna, inoltro o gateway descritta nella notifica. **Note** Il campo è visualizzato solo se alla mancata consegna è allegata una notifica sullo stato del recapito (DSN).

Destinatari del mancato recapito

Un evento di mancato recapito può riguardare uno o più destinatari. Il campo `bouncedRecipients` include il campo seguente e un elenco di oggetti, uno per ogni destinatario il cui indirizzo e-mail ha prodotto un mancato recapito.

Nome campo	Descrizione
`emailAddress`	L'indirizzo e-mail del destinatario. Se è disponibile una notifica sullo stato di consegna, questo è il valore del campo `Final-Rec ipient` della notifica.

Opzionalmente, se una notifica sullo stato di consegna è allegata al mancato recapito, possono essere presenti anche i campi seguenti.

Nome campo	Descrizione
`action`	Il valore del campo `Action` nella notifica sullo stato del recapito. Indica l'operazione eseguita dall'autorità MTA interessata come risultato del

Nome campo	Descrizione
	tentativo di recapitare il messaggio a questo destinatario.
`status`	Il valore del campo `Status` nella notifica sullo stato del recapito. Questo è il codice di stato indipendente dal trasporto che indica lo stato di consegna del messaggio per ogni destinatario.
`diagnosticCode`	Il codice di stato emesso dall'autorità MTA interessata. Si tratta del valore del campo `Diagnostic-Code` nella notifica sullo stato di consegna. Il campo potrebbe non essere incluso in questa notifica, quindi nemmeno nell'oggetto JSON.

Tipi di mancato recapito

Ogni evento di mancato recapito rientra in uno dei tipi illustrati nella tabella seguente.

Il sistema di pubblicazione degli eventi pubblica solo gli hard bounce e i soft bounce che non verranno più ritentati da Amazon SES. Quando ricevi dei mancati recapiti contrassegnati come `Permanent`, devi rimuovere i corrispondenti indirizzi e-mail dalla tua mailing list; non sarai in grado di inviare loro dei messaggi in futuro. I mancati recapiti di tipo `Transient` vengono inviati quando si verificano più soft bounce per il messaggio e Amazon SES ha smesso di tentare di consegnarli nuovamente. In futuro, potresti riuscire nuovamente a inviare messaggi a un indirizzo che inizialmente ha generato un mancato recapito `Transient`.

bounceType	bounceSubType	Descrizione
`Undetermined`	`Undetermined`	Amazon SES non è stato in grado di determinare un motivo specifico per il mancato recapito.
`Permanent`	`General`	Amazon SES ha ricevuto un mancato recapito permanente generale. Se ricevi questo tipo di mancato recapito, devi eliminare l'indirizzo e-mail del destinatario dalla lista di distribuzione.

bounceType	bounceSubType	Descrizione
`Permanent`	`NoEmail`	Amazon SES ha ricevuto un mancato recapito permanente perché l'indirizzo e-mail di destinazione non esiste. Se ricevi questo tipo di mancato recapito, devi eliminare l'indirizzo e-mail del destinatario dalla lista di distribuzione.
`Permanent`	`Suppressed`	Amazon SES non invia più a questo indirizzo perché ha una storia recente di mancati recapiti come indirizzo non valido. Per sovrascrivere l'elenco di eliminazione globale, consulta Utilizzo dell'elenco di eliminazione a livello di account di Amazon SES.
`Permanent`	`OnAccountSuppressionList`	Amazon SES ha soppresso l'invio a questo indirizzo perché si trova nell'elenco di eliminazione a livello di account. Ciò non influisce sulla metrica relativa alla frequenza dei mancati recapiti.
`Transient`	`General`	Amazon SES ha ricevuto un mancato recapito generale. È possibile che riesca a inviare messaggi a questo destinatario in futuro.
`Transient`	`MailboxFull`	Amazon SES ha ricevuto un mancato recapito per casella di posta piena. È possibile che riesca a inviare messaggi a questo destinatario in futuro.
`Transient`	`MessageTooLarge`	Amazon SES ha ricevuto un mancato recapito per messaggio troppo grande. Potresti riuscire a inviare il messaggio al destinatario riducendo le dimensioni.

bounceType	bounceSubType	Descrizione
`Transient`	`ContentRejected`	Amazon SES ha ricevuto un mancato recapito per contenuti rifiutati. Potresti riuscire a inviare il messaggio al destinatario modificandone il contenuto.
`Transient`	`AttachmentRejected`	Amazon SES ha ricevuto un mancato recapito per allegato rifiutato. Potresti riuscire a inviare il messaggio al destinatario rimuovendo o modificando l'allegato.

Oggetto del reclamo

L'oggetto JSON che contiene informazioni su un evento `Complaint` include i campi riportati di seguito.

Nome campo	Descrizione
`complainedRecipients`	Un elenco che contiene informazioni sui destinatari che potrebbero avere inviato il reclamo.
`timestamp`	La data e l'ora in cui l'ISP ha inviato la notifica di reclamo, in formato ISO8601 (AAAA-MM-GGThh:mm:ss.sZ).
`feedbackId`	Un ID univoco per il reclamo.
`complaintSubType`	Il sottotipo del reclamo, come determinato da Amazon SES.

Inoltre, se un report di feedback è associato al reclamo, potrebbero essere presenti i campi seguenti.

Nome campo	Descrizione
`userAgent`	Il valore del campo `User-Agent` nel report di feedback. Indica il nome e la versione del sistema che ha generato il report.
`complaintFeedbackType`	Il valore del campo `Feedback-Type` nel report di feedback ricevuto dall'ISP. Contiene il tipo di feedback.
`arrivalDate`	Il valore del campo `Arrival-Date` o `Received-Date` nel report di feedback, in formato ISO8601 (AAAA-MM-GGThh:mm:ss.sZ). Il campo potrebbe non essere incluso nel report, quindi nemmeno nell'oggetto JSON.

Destinatari che hanno inviato il reclamo

Il campo `complainedRecipients` contiene un elenco di destinatari che potrebbero aver inviato il reclamo.

> **Important**
>
> La maggior parte degli ISP omette gli indirizzi e-mail dei destinatari che hanno inviato reclami. Per questo motivo, il campo `complainedRecipients` include un elenco di tutti gli utenti a cui è stata inviata l'e-mail e il cui indirizzo è nel dominio che ha emesso la notifica di reclamo.

Gli oggetti JSON in questo elenco contengono il campo seguente.

Nome campo	Descrizione
`emailAddress`	L'indirizzo e-mail del destinatario.

Tipi di reclamo

Puoi visualizzare i tipi di reclamo seguenti nel campo `complaintFeedbackType`, assegnati dall'ISP che effettua la segnalazione, secondo il sito Web IANA (Internet Assigned Numbers Authority):

Nome campo	Descrizione
`abuse`	Indica un messaggio e-mail indesiderato o un altro tipo di uso illecito dell'e-mail.
`auth-failure`	Report di errore di autenticazione dell'e-mail.
`fraud`	Indica un tipo di frode o attività di phishing.
`not-spam`	Indica che l'entità che fornisce il report non considera il messaggio come spam. Può essere utilizzato per correggere un messaggio che è stato erroneamente contrassegnato o classificato come spam.
`other`	Indica qualsiasi altro feedback che non rientra in altri tipi registrati.
`virus`	Segnala la presenza di un virus nel messaggio di origine.

Sottotipi di reclami

Il valore del campo `complaintSubType` può essere null o `OnAccountSuppressionList`. Se il valore è `OnAccountSuppressionList`, Amazon SES ha accettato il messaggio, ma non ha tentato di inviarlo perché presente nell'elenco di eliminazione a livello di account.

Oggetto di consegna

L'oggetto JSON che contiene informazioni su un evento `Delivery` include i campi riportati di seguito.

Nome campo	Descrizione
`timestamp`	La data e l'ora in cui Amazon SES ha consegnato l'e-mail al server di posta del destinatario, in formato ISO8601, (AAAA-MM-GGThh:mm:ss.sZ).
`processingTimeMillis`	Il tempo in millisecondi tra quando Amazon SES ha accettato la richiesta del mittente e quando Amazon SES ha trasferito il messaggio al server di posta del destinatario.
`recipients`	Un elenco dei destinatari mirati a cui si applica l'evento di consegna.
`smtpResponse`	Il messaggio di risposta SMTP dell'ISP remoto che ha accettato l'e-mail da Amazon SES. Questo messaggio può variare in base all'e-mail, al server di posta ricevente e all'ISP ricevente.
`reportingMTA`	Il nome host del server di posta Amazon SES che ha inviato l'e-mail.

Oggetto send

L'oggetto JSON che contiene informazioni su un evento `send` è sempre vuoto.

Oggetto reject

L'oggetto JSON che contiene informazioni su un evento `Reject` include i campi riportati di seguito.

Nome campo	Descrizione
`reason`	Il motivo per cui l'e-mail è stata rifiutata. L'unico valore possibile è `Bad content`, che significa che Amazon SES ha rilevato che l'e-mail conteneva un virus. Quando un messaggio

Nome campo	Descrizione
	viene rifiutato, Amazon SES ne interrompe l'elaborazione e non tenta di inviarlo al server di posta elettronica del destinatario.

Oggetto open

L'oggetto JSON che contiene informazioni su un evento `Open` include i campi riportati di seguito.

Nome campo	Descrizione
`ipAddress`	L'indirizzo IP del destinatario.
`timestamp`	La data e l'ora in cui si è verificato l'evento apertura, in formato ISO8601 (AAAA-MM-GGThh:mm:ss.sZ).
`userAgent`	L'agente utente del dispositivo o del client di posta elettronica che il destinatario ha utilizzato per aprire l'e-mail.

Oggetto click

L'oggetto JSON che contiene informazioni su un evento `Click` include i campi riportati di seguito.

Nome campo	Descrizione
`ipAddress`	L'indirizzo IP del destinatario.
`timestamp`	La data e l'ora in cui si è verificato l'evento clic, in formato ISO8601 (AAAA-MM-GGThh:mm:ss.sZ).
`userAgent`	L'agente utente del client che il destinatario ha utilizzato per fare clic su un collegamento nell'e-mail.

Nome campo	Descrizione
`link`	L'URL del collegamento su cui il destinatario ha fatto clic.
`linkTags`	Un elenco dei tag che sono stati aggiunti al collegamento utilizzando l'attributo `ses:tags`. Per ulteriori informazioni sull'aggiunta di tag ai collegamenti nelle e-mail, consulta D5. Posso aggiungere tag ai collegamenti con identificatori univoci? in Domande frequenti sui parametri per l'invio di e-mail con Amazon SES.

Oggetto errore di rendering

L'oggetto JSON che contiene informazioni su un evento `Rendering Failure` include i campi riportati di seguito.

Nome campo	Descrizione
`templateName`	Nome del modello usato per inviare l'e-mail.
`errorMessage`	Messaggio che fornisce altre informazioni sull'errore di rendering.

Oggetto DeliveryDelay

L'oggetto JSON che contiene informazioni su un evento `DeliveryDelay` include i campi riportati di seguito.

Nome campo	Descrizione
`delayType`	Il tipo di ritardo. I valori possibili sono: • InternalFailure: un problema interno ad Amazon SES ha causato il ritardo del messaggio.

Nome campo	Descrizione
	• General: si è verificato un errore generico durante la conversazione SMTP. • MailboxFull: la casella postale del destinata rio è piena e non è in grado di ricevere messaggi aggiuntivi. • SpamDetected: il server di posta del destinatario ha rilevato una grande quantità di e-mail non richieste dal tuo account. • RecipientServerError: un problema temporaneo con il server di posta elettroni ca del destinatario impedisce il recapito del messaggio. • IPFailure: l'indirizzo IP che invia il messaggio viene bloccato od ostacolato dal provider di posta elettronica del destinatario. • TransientCommunicationFailure: si è verificat o un guasto di comunicazione temporane o durante la conversazione SMTP con il provider e-mail del destinatario. • BYOIPHostNameLookupUnavailable: Amazon SES non è riuscito a individuare il nome host DNS per gli indirizzi IP. Questo tipo di ritardo si verifica solo quando si utilizza Bring Your Own IP. • Undetermined: Amazon SES non è stato in grado di determinare il motivo del ritardo di consegna. • SendingDeferral: Amazon SES ha ritenuto opportuno posticipare internamente il messaggio.
`delayedRecipients`	Oggetto che contiene informazioni sul destinata rio del messaggio di posta elettronica.

Nome campo	Descrizione
`expirationTime`	La data e l'ora in cui Amazon SES interrompe il tentativo di recapitare il messaggio. Questo valore è mostrato in formato ISO 8601.
`reportingMTA`	Indirizzo IP dell'agente di trasferimento messaggi (MTA) che ha segnalato il ritardo.
`timestamp`	La data e l'ora in cui si è verificato il ritardo, mostrate in formato ISO 8601.

Destinatari del ritardo di consegna

L'oggetto `delayedRecipients` include i seguenti valori.

Nome campo	Descrizione
`emailAddress`	Indirizzo di posta elettronica che ha provocato un ritardo nel recapito del messaggio.
`status`	Il codice di stato SMTP associato al ritardo di consegna.
`diagnosticCode`	Il codice diagnostico fornito dal Message Transfer Agent (MTA) ricevente.

Oggetto sottoscrizione

L'oggetto JSON che contiene informazioni su un evento `Subscription` include i campi riportati di seguito.

Nome campo	Descrizione
`contactList`	Il nome dell’elenco in cui si trova il contatto.

Nome campo	Descrizione
`timestamp`	La data e l'ora in cui l'ISP ha inviato la notifica di sottoscrizione, in formato ISO8601 (AAAA-MM-GGThh:mm:ss.sZ).
`source`	L'indirizzo e-mail da cui il messaggio è stato inviato (indirizzo MAIL FROM della busta).
`newTopicPreferences`	Una struttura dati JSON (mappa) che specifica lo stato della sottoscrizione di tutti gli argomenti dell'elenco dei contatti che indicano lo stato dopo una modifica (contatto sottoscritto o annullato).
`oldTopicPreferences`	Una struttura dati JSON (mappa) che specifica lo stato della sottoscrizione di tutti gli argomenti dell'elenco dei contatti che indicano lo stato prima della modifica (contatto sottoscritto o annullato).

Preferenze per argomento nuovo/vecchio

Gli oggetti `newTopicPreferences` e `oldTopicPreferences` includono i seguenti valori.

Nome campo	Descrizione
`unsubscribeAll`	Specifica se il contatto ha annullato la sottoscrizione a tutti gli argomenti dell'elenco dei contatti.
`topicSubscriptionStatus`	Specifica l'argomento nel campo `topicName` e mappa lo stato di sottoscrizione (OptIn oppure OptOut) nel campo `subscriptionStatus`.
`topicDefaultSubscriptionStatus`	Specifica l'argomento nel campo `topicName` e mappa lo stato di sottoscrizione (OptIn

Nome campo	Descrizione
	oppure OptOut) nel campo `subscriptionStatus` .

Esempi di dati degli eventi pubblicati da Amazon SES su Amazon SNS

In questa sezione vengono forniti esempi dei vari tipi di record di eventi di invio di e-mail che Amazon SES pubblica in Amazon SNS.

Argomenti in questa sezione:

- Record di eventi di mancato recapito
- Record di eventi di reclamo
- Record di eventi di consegna
- Record di eventi di invio
- Record di eventi di rifiuto
- Record di eventi di apertura
- Record di eventi di clic
- Record di eventi di errore di rendering
- DeliveryDelayrecord
- Registro di sottoscrizione

> **Note**
>
> Negli esempi in cui si utilizza un campo `tag`, utilizza la pubblicazione di eventi attraverso un set di configurazione per il quale SES supporta la pubblicazione di tag per tutti i tipi di evento. Se utilizzi le notifiche di feedback direttamente sull'identità, SES non pubblica tag. Ottieni ulteriori informazioni sull'aggiunta di tag durante la creazione di un set di configurazione o la modifica di un set di configurazione.

Record di eventi di mancato recapito

Di seguito è riportato un esempio di record di eventi `Bounce` che Amazon SES pubblica in 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"
      ]
    }
  }
}
```

Record di eventi di reclamo

Di seguito è riportato un esempio di record di eventi `Complaint` che Amazon SES pubblica in 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"
      ]
    }
  }
}
```

Record di eventi di consegna

Di seguito è riportato un esempio di record di eventi `Delivery` che Amazon SES pubblica in 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"
  }
}
```

Record di eventi di invio

Di seguito è riportato un esempio di record di eventi `Send` che Amazon SES pubblica in Amazon SNS. Alcuni campi non sono sempre presenti. Ad esempio, con un'e-mail con modelli, l'oggetto viene visualizzato in un secondo momento e incluso negli eventi successivi.

```
{
  "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": {}
}
```

Record di eventi di rifiuto

Di seguito è riportato un esempio di record di eventi `Reject` che Amazon SES pubblica in 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"
  }
}
```

Record di eventi di apertura

Di seguito è riportato un esempio di record di eventi 0pen che Amazon SES pubblica in 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"
  }
}
```

Record di eventi di clic

Di seguito è riportato un esempio di record di eventi `Click` che Amazon SES pubblica in 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"
  }
}
```

Record di eventi di errore di rendering

Di seguito è riportato un esempio di record di eventi `Rendering Failure` che Amazon SES pubblica in 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"
  }
}
```

DeliveryDelayrecord

Di seguito è riportato un esempio di record di eventi `DeliveryDelay` che Amazon SES pubblica in 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 di sottoscrizione

Di seguito è riportato un esempio di record di `Subscription` eventi che Amazon SES pubblica su 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"
        }
      ]
    }
  }
}
```

Monitoraggio della reputazione del mittente Amazon SES

Amazon SES tiene traccia attivamente di diversi parametri che possono danneggiare la tua reputazione di mittente o provocare una riduzione delle percentuali di consegna delle e-mail. Due importanti parametri considerati in questo processo sono le percentuali di mancati recapiti e di reclami per l'account. Se la percentuale di mancato recapito o reclamo per il tuo account è troppo elevato, potremmo mettere il tuo account in fase di verifica o sospendere la capacità del tuo account di inviare e-mail.

Poiché la percentuale di mancati recapiti e reclami è molto importante per lo stato di integrità dell'account, Amazon SES include una pagina di parametri della reputazione nella console Amazon SES che permette di monitorare questi parametri. I parametri sulla reputazione permettono anche di visualizzare informazioni su fattori non correlati a mancati recapiti o reclami che potrebbero danneggiare la reputazione di mittente. Se, ad esempio, invii e-mail a un indirizzo spamtrap noto, in questo pannello di controllo viene visualizzato un messaggio.

Questa sezione contiene informazioni relative all'accesso ai parametri sulla reputazione, all'interpretazione delle informazioni contenute e alla configurazione dei sistemi per l'invio di notifiche relative ai fattori che possono influire sulla reputazione di mittente.

In questa sezione vengono trattati gli argomenti seguenti:

- Utilizzo dei parametri sulla reputazione per tenere traccia delle percentuali di mancati recapiti e reclami
- Messaggi sui parametri di reputazione
- Creazione di allarmi di monitoraggio della reputazione tramite CloudWatch
- Parametri SNDS per gli indirizzi IP dedicati
- Sospensione automatica dell'invio di e-mail

Utilizzo dei parametri sulla reputazione per tenere traccia delle percentuali di mancati recapiti e reclami

La pagina della console sui parametri di reputazione contiene le stesse informazioni che il team Amazon SES esamina per determinare lo stato di integrità dei singoli account.

Visualizzazione dei parametri di reputazione

1. Accedi alla AWS Management Console e apri la console Amazon SES all'indirizzo https://console.aws.amazon.com/ses/.
2. Nel pannello di navigazione sul lato sinistro dello schermo, scegli Reputation metrics (Parametri di reputazione).

   Il pannello di controllo visualizza le informazioni riportate di seguito.

   - Account status (Stato dell'account): un riepilogo dello stato di integrità delle percentuali di mancati recapiti e reclami. I valori possibili includono:
     - Healthy (Integro): attualmente non ci sono problemi relativi all'account.
     - Under review (In fase di verifica): il tuo account è in fase di verifica. Se i problemi che hanno determinato la verifica del tuo account non vengono risolti entro la fine del periodo di verifica, potremmo sospendere la capacità del tuo account di inviare e-mail.
     - Pending end of review decision (In attesa di decisione dopo la verifica): l'account è in prova. A causa del tipo di problemi che ci hanno indotto alla verifica del tuo account, dobbiamo eseguire una verifica manuale del tuo account prima di eseguire altre operazioni.
     - Sending paused (Invio sospeso): abbiamo sospeso la capacità del tuo account di inviare e-mail. Durante la sospensione della capacità del tuo account di inviare e-mail, non potrai inviare e-mail utilizzando Amazon SES. Puoi richiederci la verifica di tale decisione. Per ulteriori informazioni sulla richiesta di riesame, consulta Domande frequenti sul processo di verifica dell'invio di Amazon SES.
     - Pending sending pause (Sospensione dell'invio pendente): il tuo account è in fase di verifica. I problemi che ci hanno indotto alla verifica del tuo account non sono stati risolti. In tali casi, in genere sospendiamo la capacità del tuo account di inviare e-mail. A causa della natura dell'account, tuttavia, dobbiamo verificare il tuo account prima di eseguire qualsiasi ulteriore operazione.
   - Bounce Rate (Percentuale di mancati recapiti): la percentuale di e-mail inviate dal tuo account che hanno generato un mancato recapito permanente. Consulta la pagina che illustra come viene calcolata la percentuale di mancati recapiti.
   - Complaint Rate (Percentuale di reclami): la percentuale di e-mail inviate dal tuo account che i destinatari hanno segnalato come spam. Consulta la pagina che illustra come viene calcolata la percentuale di reclami

> **Note**
>
> Le sezioni Bounce Rate (Percentuale di mancati recapiti) e Complaint Rate (Percentuale di reclami) includono anche messaggi di stato per i rispettivi parametri. Di seguito è riportato un elenco di messaggi di stato che possono apparire per questi parametri:
>
> - Healthy (Integro): il parametro rientra nei livelli normali.
> - Almost healed (Quasi risanato): il parametro ha causato la messa in fase di verifica dell'account. Poiché il periodo di verifica è iniziato, il parametro è rimasto al di sotto della percentuale massima. Se il parametro rimane al di sotto della percentuale massima, lo stato relativo passa a Healthy (Integro) prima del termine del periodo di verifica.
> - Under review (In fase di verifica): il parametro ha causato la verifica dell'account ed è ancora al di sopra della percentuale massima. Se i problemi che hanno determinato il superamento della percentuale massima da parte del parametro non vengono risolti entro la fine del periodo di verifica, potremmo sospendere la capacità del tuo account di inviare e-mail.
> - Sending pause (Sospensione dell'invio): il parametro ci ha indotti a sospendere la capacità del tuo account di inviare e-mail. Durante la sospensione della capacità del tuo account di inviare e-mail, non puoi inviare e-mail utilizzando Amazon SES. Puoi richiederci la verifica di tale decisione. Per ulteriori informazioni sulla presentazione di una richiesta di riesame, consulta Domande frequenti sul processo di verifica dell'invio di Amazon SES.
> - Pending sending pause (Sospensione dell'invio pendente): il parametro ci ha indotti a porre il tuo account in fase di verifica. I problemi che hanno causato la messa in fase di verifica non sono stati risolti. Questi problemi potrebbero determinare la sospensione della capacità del tuo account di inviare e-mail. Un membro del team di Amazon SES verificherà l'account prima di qualsiasi ulteriore operazione.

- Other Notifications (Altre notifiche): se il tuo account sta avendo problemi di reputazione non correlati a mancati recapiti o reclami, qui verrà visualizzato un breve messaggio. Per ulteriori informazioni sulle notifiche che possono essere visualizzate in quest'area, consulta Messaggi sui parametri di reputazione.

Messaggi sui parametri di reputazione

La pagina sulla console delle parametri di reputazione Amazon SES fornisce importanti parametri correlati al tuo account. Le seguenti sezioni descrivono i messaggi che potrebbero essere visualizzati in questo pannello di controllo e forniscono consigli e informazioni che puoi utilizzare per risolvere i problemi correlati alla tua reputazione di mittente.

Questa sezione contiene informazioni sui seguenti tipi di notifiche:

- Messaggi di stato
- Notifica della percentuale di mancati recapiti (bounce)
- Notifica della percentuale di reclami
- Notifica delle organizzazioni antispam
- Notifica tramite listbombing
- Notifica di feedback diretto
- Notifica di elenco di domini bloccati
- Notifica di revisione interna
- Notifica di fornitori di mailbox
- Notifica di feedback dei destinatari
- Notifica di account correlato
- Notifica di spamtrap
- Notifica di sito vulnerabile
- Notifica contro le credenziali compromesse
- Notifica di altro tipo

Messaggi di stato

Quando utilizzi il pannello di controllo sulla reputazione, vedrai un messaggio che descrive lo stato del tuo account Amazon SES. Di seguito è riportato un elenco di possibili valori dello stato dell'account:

- Healthy (Integro): attualmente non ci sono problemi relativi all'account.

- Under review (In fase di verifica): il tuo account è in fase di verifica. Se i problemi che hanno determinato la verifica del tuo account non vengono risolti entro la fine del periodo di verifica, potremmo sospendere la capacità del tuo account di inviare e-mail.
- Pending end of review decision (In attesa di decisione dopo la verifica): l'account è in prova. A causa del tipo di problemi che ci hanno indotto alla verifica del tuo account, dobbiamo eseguire una verifica manuale del tuo account prima di eseguire altre operazioni.
- Sending paused (Invio sospeso): abbiamo sospeso la capacità del tuo account di inviare e-mail. Durante la sospensione della capacità del tuo account di inviare e-mail, non potrai inviare e-mail utilizzando Amazon SES. Puoi richiederci la verifica di tale decisione. Per ulteriori informazioni sulla richiesta di riesame, consulta Domande frequenti sul processo di verifica dell'invio di Amazon SES.
- Pending sending pause (Sospensione dell'invio pendente): il tuo account è in fase di verifica. I problemi che ci hanno indotto alla verifica del tuo account non sono stati risolti. In tali casi, in genere sospendiamo la capacità del tuo account di inviare e-mail. A causa della natura dell'account, tuttavia, dobbiamo verificare il tuo account prima di eseguire qualsiasi ulteriore operazione.

Inoltre, le sezioni Bounce Rate (Percentuale di mancati recapiti) e Complaint Rate (Percentuale di reclami) della pagina sui parametri di reputazione mostrano lo stato che riepiloga i rispettivi parametri. Di seguito è riportato un elenco di possibili valori dello stato dei parametri:

- Healthy (Integro): il parametro rientra nei livelli normali.
- Almost healed (Quasi risanato): il parametro ha causato la messa in fase di verifica dell'account. Poiché il periodo di verifica è iniziato, il parametro è rimasto al di sotto della percentuale massima. Se il parametro rimane al di sotto della percentuale massima, lo stato relativo passa a Healthy (Integro) prima del termine del periodo di verifica.
- Under review (In fase di verifica): il parametro ha causato la verifica dell'account ed è ancora al di sopra della percentuale massima. Se i problemi che hanno determinato il superamento della percentuale massima da parte del parametro non vengono risolti entro la fine del periodo di verifica, potremmo sospendere la capacità del tuo account di inviare e-mail.
- Sending pause (Sospensione dell'invio): il parametro ci ha indotti a sospendere la capacità del tuo account di inviare e-mail. Durante la sospensione della capacità del tuo account di inviare e-mail, non puoi inviare e-mail utilizzando Amazon SES. Puoi richiederci la verifica di tale decisione. Per ulteriori informazioni sulla presentazione di una richiesta di riesame, consulta Domande frequenti sul processo di verifica dell'invio di Amazon SES.

- Pending sending pause (Sospensione dell'invio pendente): il parametro ci ha indotti a porre il tuo account in fase di verifica. I problemi che hanno causato la messa in fase di verifica non sono stati risolti. Questi problemi potrebbero determinare la sospensione della capacità del tuo account di inviare e-mail. Un membro del team di Amazon SES verificherà l'account prima di qualsiasi ulteriore operazione.

Notifica della percentuale di mancati recapiti (bounce)

Questa sezione contiene ulteriori informazioni sulle notifiche della percentuale di mancati recapiti mostrate nella pagina dei parametri di reputazione Amazon SES.

Perché hai ricevuto questa notifica

Hai ricevuto questa notifica perché la frequenza di mancati recapiti per il tuo account era troppo alta. La percentuale di mancati recapiti si basa sul numero di mancati recapiti permanenti generati dall'account Amazon SES. La maggior parte dei provider di posta elettronica interpreta un'elevata percentuale di mancati recapiti come indice del fatto che un mittente non gestisce correttamente l'elenco dei destinatari e che potrebbe inviare e-mail non richieste.

Un hard bounce, o mancato recapito permanente, si verifica quando un'e-mail viene inviata a un indirizzo che non esiste. Amazon SES non considera i soft bounce (e-mail non recapitata), cioè i mancati recapiti dovuti al fatto che l'indirizzo di un destinatario non è temporaneamente in grado di ricevere il messaggio, in questo calcolo. Anche le e-mail non recapitate inviate a indirizzi e domini verificati, così come le e-mail inviate al simulatore di posta in arrivo Amazon SES, non sono considerate in questo calcolo.

Calcoliamo la tua frequenza di mancati recapiti in base a un volume rappresentativo di e-mail. Il volume rappresentativo è il numero di e-mail che rappresenta la tua tipica prassi di invio. Per ottenere un risultato equo tra mittenti a volume elevato e a volume ridotto, il volume rappresentativo è diverso per ogni utente e cambia con il mutare dei pattern di invio dell'utente.

Per ottenere i migliori risultati, mantenere una frequenza di mancati recapiti inferiore al 5%. Percentuali di mancati recapiti superiori possono influire sulla consegna delle e-mail. Se la percentuale di mancati recapiti è del 5% o superiore, l'account viene messo automaticamente in fase di revisione. Se la percentuale di mancati recapiti è del 10% o superiore, la capacità dell'account di inviare ulteriori e-mail potrebbe essere sospesa finché il problema che ha causato l'elevata percentuale di mancati recapiti non è stato risolto.

Cosa puoi fare per risolvere il problema

Se non lo hai già fatto, stabilisci un processo per acquisire e gestire i mancati recapiti e i reclami. Tutti gli account Amazon SES devono obbligatoriamente adottare questi processi. Per ulteriori informazioni, consulta Parametri di riuscita del programma e-mail.

Individua quindi gli indirizzi e-mail che provocano i mancati recapiti e crea e implementa un piano per ridurre o eliminare questi ultimi. Se la possibilità dell'account di inviare e-mail è già stata sospesa, accedi all'AWS Management Console e vai sull'AWS Support. Rispondi al caso che abbiamo aperto per tuo conto.

Se il tuo account è in fase di verifica

Se alla fine del periodo di verifica la percentuale di mancato recapito del tuo account resta al di sopra del 10%, potremmo sospendere la capacità del tuo account di inviare e-mail.

Se hai effettuato delle modifiche che ritieni possano risolvere il problema, accedi alla console AWS e vai nel Centro assistenza. Rispondi al caso che abbiamo aperto per tuo conto. Nella risposta alla pratica, descrivi le modifiche che hai implementato. Se concorderemo che le modifiche possono ridurre la percentuale di mancati recapiti, modificheremo i calcoli in modo da considerare solo i mancati recapiti ricevuti dopo l'implementazione delle modifiche.

Sospensione della capacità del tuo account di inviare e-mail

Puoi chiederci di rivedere tale decisione. Per ulteriori informazioni, consulta Domande frequenti sul processo di verifica dell'invio di Amazon SES.

Se implementi delle modifiche che ritieni possano risolvere il problema, accedi alla console AWS e vai nel Centro assistenza. Rispondi al caso che abbiamo aperto per tuo conto. Includi i dettagli delle azioni intraprese per risolvere il problema, nonché i dettagli dei piani volti ad assicurare che questo problema non si verifichi nuovamente. Dopo aver ricevuto la tua richiesta, esaminiamo le informazioni che hai fornito e modifichiamo lo stato del tuo account, se necessario.

Notifica della percentuale di reclami

Questa sezione contiene ulteriori informazioni sulle notifiche della percentuale di reclami mostrate nella pagina dei parametri di reputazione Amazon SES.

Perché hai ricevuto questa notifica

Hai ricevuto questa notifica perché la percentuale di reclami per il tuo account era troppo alta. La percentuale di reclami si basa sul numero di reclami generati dal tuo account Amazon SES. La maggior parte dei provider di posta elettronica interpreta un'elevata percentuale di reclami come indice del fatto che un mittente non gestisce correttamente l'elenco dei destinatari e che potrebbe inviare e-mail non richieste.

Un reclamo si verifica quando un destinatario identifica un'e-mail che hai inviato come posta indesiderata. Questo di solito si verifica quando il destinatario utilizza il pulsante Segnala spam nel proprio client di posta elettronica. I reclami generati dai messaggi di posta elettronica inviati al simulatore di posta in arrivo Amazon SES non vengono considerati in questo calcolo.

Calcoliamo la tua percentuale di reclami in base a un volume rappresentativo di e-mail. Il volume rappresentativo è il numero di e-mail che rappresenta la tua tipica prassi di invio. Per ottenere un risultato equo tra mittenti a volume elevato e a volume ridotto, il volume rappresentativo è diverso per ogni utente e cambia con il mutare dei pattern di invio dell'utente.

Per ottenere i migliori risultati, mantenere un tasso di reclami inferiore allo 0,1%. Percentuali di reclami superiori possono influire sulla consegna delle e-mail. Se la percentuale di reclami è dello 0,1% o superiore, l'account viene messo automaticamente in fase di revisione. Se la percentuale di reclami è dello 0,5% o superiore, la capacità dell'account di inviare ulteriori e-mail potrebbe essere sospesa finché il problema che ha causato l'elevata percentuale di reclami non è stato risolto.

Cosa puoi fare per risolvere il problema

Se non lo hai già fatto, stabilisci un processo per acquisire e gestire i mancati recapiti e i reclami. Tutti gli account Amazon SES devono obbligatoriamente adottare questi processi. Per ulteriori informazioni, consulta Parametri di riuscita del programma e-mail.

Individua quindi i messaggi che invii che provocano i reclami e implementa un piano per ridurre questi ultimi. Se la possibilità dell'account di inviare e-mail è già stata sospesa, accedi alla console AWS e vai al Centro assistenza. Rispondi alla pratica che abbiamo aperto per tuo conto

Devi immediatamente interrompere l'invio agli indirizzi da cui provengono i reclami, ma allo stesso tempo è importante che identifichi i fattori che provocano tali reclami. Dopo aver identificato questi fattori, neutralizzali modificando il tuo comportamento di invio di e-mail.

Se il tuo account è in fase di verifica

Se alla fine del periodo di verifica la percentuale di reclami del tuo account resta al di sopra dello 0,5%, potremmo sospendere la capacità del tuo account di inviare e-mail.

Se hai effettuato delle modifiche che ritieni possano risolvere il problema, accedi alla console AWS e vai nel Centro assistenza. Rispondi al caso che abbiamo aperto per tuo conto. Nella risposta alla pratica, descrivi le modifiche che hai implementato. Se concorderemo che le modifiche possono ridurre la percentuale di reclami, modificheremo i calcoli in modo da considerare solo i reclami ricevuti dopo l'implementazione delle modifiche.

Sospensione della capacità del tuo account di inviare e-mail

Puoi chiederci di rivedere tale decisione. Per ulteriori informazioni, consulta Domande frequenti sul processo di verifica dell'invio di Amazon SES.

Quando hai effettuato le modifiche che ritieni possano risolvere il problema, accedi alla console AWS e vai nel Centro assistenza. Rispondi al caso che abbiamo aperto per tuo conto. Includi i dettagli delle azioni intraprese per risolvere il problema, nonché i dettagli dei piani volti ad assicurare che questo problema non si verifichi nuovamente. Dopo aver ricevuto la tua richiesta, esaminiamo le informazioni che hai fornito e modifichiamo lo stato del tuo account, se necessario.

Notifica delle organizzazioni antispam

Questa sezione contiene ulteriori informazioni sulle notifiche delle organizzazioni antispam mostrate nella pagina dei parametri di reputazione Amazon SES.

Perché hai ricevuto questa notifica

Un'organizzazione antispam attendibile ha segnalato che alcuni dei contenuti inviati dal tuo account Amazon SES sono stati contrassegnati come non richiesti o problematici dal loro sistema.

Non siamo in grado di fornire informazioni sui messaggi specifici che hanno causato l'indicazione dei contenuti da parte dell'organizzazione di protezione da posta indesiderata. Non possiamo fornire il nome dell'organizzazione che ha emesso il report. Di solito, le organizzazioni antispam considerano una combinazione dei seguenti fattori: feedback del destinatario, parametri di coinvolgimento del messaggio, tentativi di consegna a indirizzi non validi, contenuti contrassegnati dai loro filtri antispam e numero di accessi a trappole per spam. Questo non è un elenco esaustivo; Altri fattori potrebbero indurre queste organizzazioni a contrassegnare i tuoi contenuti.

Cosa puoi fare per risolvere il problema

Per risolvere questo problema, devi determinare quali aspetti del tuo programma di invio di e-mail potrebbero indurre l'organizzazione antispam a contrassegnare le e-mail come problematiche. Devi quindi modificare il programma di invio per risolvere i problemi individuati.

Se il tuo account è in fase di verifica

Alla fine del periodo di verifica, se l'organizzazione antispam continua a identificare le e-mail inviate dal tuo account come problematiche, potremmo sospendere la capacità del tuo account di inviare e-mail finché non risolvi il problema.

Se hai effettuato delle modifiche che ritieni possano risolvere il problema, accedi alla console AWS e vai nel Centro assistenza. Rispondi al caso che abbiamo aperto per tuo conto. Nel tuo messaggio, fornisci i dettagli delle modifiche apportate. Una volta ricevute queste informazioni, estenderemo il periodo di verifica per assicurarci di analizzare solo le notifiche dell'organizzazione antispam ricevute dopo che hai implementato le modifiche. Al termine di questa estensione del periodo di verifica, se il tuo account non viene più segnalato dall'organizzazione antispam, rimuoveremo lo stato di verifica dal tuo account.

Sospensione della capacità del tuo account di inviare e-mail

Puoi chiederci di rivedere tale decisione. Per ulteriori informazioni, consulta Domande frequenti sul processo di verifica dell'invio di Amazon SES.

Quando hai effettuato le modifiche che ritieni possano risolvere il problema, accedi alla console AWS e vai nel Centro assistenza. Rispondi al caso che abbiamo aperto per tuo conto. Includi i dettagli delle azioni intraprese per risolvere il problema, nonché i dettagli dei piani volti ad assicurare che questo problema non si verifichi nuovamente. Dopo aver ricevuto la tua richiesta, esaminiamo le informazioni che hai fornito e modifichiamo lo stato del tuo account, se necessario.

Notifica tramite listbombing

Questa sezione contiene ulteriori informazioni sulle notifiche di listbombing mostrate nella pagina delle metriche di reputazione Amazon SES.

Perché hai ricevuto questa notifica

Un'organizzazione anti-spam ha identificato che i tuoi processi di invio di e-mail sono vulnerabili al «listbombing». Il listbombing è una forma di abuso in cui un malintenzionato registra un numero molto

elevato di indirizzi e-mail su un modulo basato sul Web. Il listbombing può causare interruzioni del servizio per gli utenti dei servizi di posta elettronica interessati. Può anche comportare il blocco della posta elettronica da parte dei provider di posta elettronica.

Le organizzazioni anti-spam utilizzano metodi proprietari per identificare i siti vulnerabili al listbombing. Per questo motivo, non possiamo fornire ulteriori dettagli sul problema che ha portato l'organizzazione anti-spam a identificare il tuo processo di invio e-mail come problematico. Non possiamo fornire il nome dell'organizzazione che ha identificato il problema.

Cosa puoi fare per risolvere il problema

Dovresti esaminare tutti i moduli di iscrizione basati sul Web per assicurarti che non siano vulnerabili a questo tipo di abuso. Ogni modulo dovrebbe includere un CAPTCHA per impedire agli script automatici di inviare richieste di abbonamento. Inoltre, quando i nuovi utenti si iscrivono al tuo prodotto o servizio, invia loro un'e-mail per confermare che, di fatto, intendevano iscriversi. Non inviare alcuna e-mail aggiuntiva ai clienti a meno che non scelgano esplicitamente di adertire alle tue comunicazioni.

Infine, dovresti eseguire un «pass di autorizzazione» nella tua lista e-mail. In un pass di autorizzazione, invii un'e-mail a tutti i tuoi clienti chiedendo loro se vogliono ancora ricevere e-mail da te. Invia e-mail solo ai clienti che confermano di voler continuare a ricevere e-mail da te.

Se il tuo account è in fase di verifica

Alla fine del periodo di verifica, se l'organizzazione antispam continua a identificare le e-mail inviate dal tuo account come problematiche, potremmo sospendere la capacità del tuo account di inviare e-mail finché non risolvi il problema.

Se hai effettuato delle modifiche che ritieni possano risolvere il problema, accedi alla console AWS e vai nel Centro assistenza. Rispondi al caso che abbiamo aperto per tuo conto. Nel tuo messaggio, fornisci i dettagli delle modifiche apportate. Una volta ricevute queste informazioni, estenderemo il periodo di verifica per assicurarci di analizzare solo le notifiche dell'organizzazione antispam ricevute dopo che hai implementato le modifiche. Al termine di questa estensione del periodo di verifica, se il tuo account non viene più segnalato dall'organizzazione antispam, rimuoveremo lo stato di verifica dal tuo account.

Sospensione della capacità del tuo account di inviare e-mail

Puoi chiederci di rivedere tale decisione. Per ulteriori informazioni, consulta Domande frequenti sul processo di verifica dell'invio di Amazon SES.

Quando hai effettuato le modifiche che ritieni possano risolvere il problema, accedi alla console AWS e vai nel Centro assistenza. Rispondi al caso che abbiamo aperto per tuo conto. Includi i dettagli delle azioni intraprese per risolvere il problema, nonché i dettagli dei piani volti ad assicurare che questo problema non si verifichi nuovamente. Dopo aver ricevuto la tua richiesta, esaminiamo le informazioni che hai fornito e modifichiamo lo stato del tuo account, se necessario.

Notifica di feedback diretto

Questa sezione contiene ulteriori informazioni sulle notifiche di feedback diretto mostrate nella pagina dei parametri di reputazione Amazon SES.

Perché hai ricevuto questa notifica

Un notevole numero di utenti ha contattato Amazon SES direttamente per segnalare messaggi ricevuti da un indirizzo o dominio associato al tuo account Amazon SES. Questo tipo di feedback non è visibile nei reclami segnalati direttamente dai fornitori di mailbox e non è incluso nei parametri dei mancati recapiti e reclami visualizzati nella pagina dei parametri di reputazione.

Per proteggere la privacy degli utenti che hanno segnalato questi problemi, non possiamo fornire i loro indirizzi e-mail.

I destinatari possono reclamare con Amazon SES quando ricevono messaggi per cui non si sono registrati, quando non ricevono il tipo di e-mail che prevedevano di ricevere, quando non ritengono che le e-mail ricevute siano utili o interessanti, quando non riconoscono i messaggi come l'oggetto della loro registrazione oppure quando ricevono troppi messaggi. Non si tratta di un elenco esaustivo, I fattori pertinenti al tuo caso dipendono dal tuo specifico programma di invio di e-mail.

Cosa puoi fare per risolvere il problema

Consigliamo di implementare una strategia con doppio consenso esplicito per acquisire nuovi indirizzi, come descritto in Creazione e gestione degli elenchi, e di inviare e-mail solo agli indirizzi che completano il processo di doppio consenso.

Inoltre, dovresti eliminare gli elenchi di indirizzi che non hanno interagito con le tue e-mail di recente. Puoi utilizzare il tracciamento di apertura e clic, come descritto in Monitoraggio delle attività di invio di Amazon SES, per determinare quali utenti visualizzano e interagiscono con il contenuto inviato.

Se il tuo account è in fase di verifica

Alla fine del periodo di verifica, se Amazon SES continua a ricevere un numero rilevante di reclami diretti in relazione ai messaggi inviati dal tuo account, potremmo sospendere la capacità del tuo account di inviare e-mail finché non risolvi il problema.

Se hai effettuato delle modifiche che ritieni possano risolvere il problema, accedi alla console AWS e vai nel Centro assistenza. Rispondi al caso che abbiamo aperto per tuo conto. Fornisci informazioni dettagliate sulle operazioni che hai effettuato per risolvere il problema e descrivi in che modo tali interventi potranno evitare che il problema si ripeta in futuro. Se riteniamo che le modifiche apportate possano risolvere in modo appropriato il problema, annulliamo il periodo di verifica del tuo account.

Sospensione della capacità del tuo account di inviare e-mail

Puoi chiederci di rivedere tale decisione. Per ulteriori informazioni, consulta Domande frequenti sul processo di verifica dell'invio di Amazon SES.

Quando hai effettuato le modifiche che ritieni possano risolvere il problema, accedi alla console AWS e vai nel Centro assistenza. Rispondi al caso che abbiamo aperto per tuo conto. Includi i dettagli delle azioni intraprese per risolvere il problema, nonché i dettagli dei piani volti ad assicurare che questo problema non si verifichi nuovamente. Dopo aver ricevuto la tua richiesta, esaminiamo le informazioni che hai fornito e modifichiamo lo stato del tuo account, se necessario.

Notifica di elenco di domini bloccati

Questa sezione contiene ulteriori informazioni sulle notifiche di elenco di domini bloccati mostrate nella pagina dei parametri di reputazione Amazon SES.

Perché hai ricevuto questa notifica

Le e-mail inviate dal tuo account Amazon SES contengono riferimenti a domini che sono stati inclusi in un elenco attendibile di domini bloccati. I domini in questo tipo di elenco sono in genere associati a comportamenti illeciti o dannosi. I domini in questione possono essere o meno i domini da cui stai inviando le tue e-mail. Possono essere contrassegnati anche i messaggi che includono riferimenti o collegamenti a un dominio incluso in uno di questi elenchi o che includono immagini ospitate su tali domini.

Non siamo in grado di fornire i nomi dei domini che causano la segnalazione dei tuoi messaggi, né di identificare le-mail contrassegnate in questo modo.

Cosa puoi fare per risolvere il problema

Innanzitutto, crea un elenco di tutti i domini a cui si fa riferimento nelle e-mail inviate tramite Amazon SES. Successivamente, utilizza lo strumento Spamhaus Domain Lookup per determinare quali domini nel tuo messaggio di posta elettronica si trovano nel blocklist del dominio. In tale elenco potrebbero essere presenti più domini a cui fai riferimento nelle tue e-mail.

Spamhaus Domain Blocklist non è affiliato con Amazon SES o AWS. Non forniamo alcuna garanzia circa l'accuratezza dei domini in questo elenco. Gli strumenti Spamhaus Domain Blocklist e Domain Lookup sono di proprietà di Spamhaus Project, che ne cura anche la gestione e la manutenzione.

Se il tuo account è in fase di verifica

Cerchiamo riferimenti a domini utilizzati per scopi dannosi nelle e-mail inviate durante il periodo di revisione. Se le tue e-mail contengono ancora un numero significativo di riferimenti a questi domini, potremmo sospendere la capacità del tuo account di inviare e-mail fino a quando non risolvi il problema.

Se hai effettuato delle modifiche che ritieni possano risolvere il problema, accedi alla console AWS e vai nel Centro assistenza. Rispondi al caso che abbiamo aperto per tuo conto. Nel tuo messaggio, fornisci i dettagli delle modifiche apportate. Una volta ricevute queste informazioni, estenderemo il periodo di verifica per assicurarci di analizzare solo il numero di domini bloccati presenti nelle tue e-mail dopo che hai implementato le modifiche. Al termine di questa estensione del periodo di verifica, se il numero di notifiche della blocklist del dominio è stato ridotto o eliminato e riteniamo che hai adottato misure atte a evitare che questo problema si verifichi nuovamente in futuro, annulleremo il periodo di verifica per il tuo account.

Sospensione della capacità del tuo account di inviare e-mail

Puoi chiederci di rivedere tale decisione. Per ulteriori informazioni, consulta Domande frequenti sul processo di verifica dell'invio di Amazon SES.

Quando hai effettuato le modifiche che ritieni possano risolvere il problema, accedi alla console AWS e vai nel Centro assistenza. Rispondi al caso che abbiamo aperto per tuo conto. Includi i dettagli delle azioni intraprese per risolvere il problema, nonché i dettagli dei piani volti ad assicurare che questo problema non si verifichi nuovamente. Dopo aver ricevuto la tua richiesta, esaminiamo le informazioni che hai fornito e modifichiamo lo stato del tuo account, se necessario.

Notifica di revisione interna

Questa sezione contiene ulteriori informazioni sulle notifiche di revisione interna mostrate nella pagina dei parametri di reputazione Amazon SES.

Perché hai ricevuto questa notifica

Una revisione completa del tuo account ha individuato alcune caratteristiche che potrebbero indurre i fornitori di mailbox o i destinatari a identificare i tuoi messaggi come spam.

Per proteggere il nostro processo di rilevamento di uso illecito, non possiamo rivelare i fattori specifici che hanno portato a contrassegnare il tuo account in questo modo.

Fattori comuni che possono condurre a questa determinazione includono i seguenti:

- messaggi contrassegnati da sistemi antispam commerciali;
- contenuto del messaggio che implica che il destinatario non ha esplicitamente richiesto l'e-mail;
- mancata corrispondenza tra il mittente del messaggio e il marchio nel corpo dell'e-mail;
- contenuto che non evidenzia chi sia il mittente;
- invio di messaggi che riguardano contenuti associati e-mail non richieste;
- schemi di formattazione associati a e-mail non richieste;
- invio da domini o riferimento a domini con scarsa reputazione.

Questo non è un elenco completo. Il motivo specifico di questa notifica potrebbe essere una combinazione di questi fattori oppure un fattore non elencato.

Cosa puoi fare per risolvere il problema

I seguenti suggerimenti potrebbero aiutarti a ridurre la gravità del problema:

- Assicurati che i destinatari che stai contattando siano solo quelli che hanno esplicitamente chiesto di ricevere e-mail da te.
- Non acquistare, noleggiare o prendere a prestito elenchi di destinatari di e-mail.
- Non tentare di nascondere la tua identità o lo scopo della tua comunicazione nei messaggi inviati.
- Crea un elenco di tutti i domini referenziati nelle e-mail che invii mediante Amazon SES, quindi usa lo strumento di ricerca dei domini di Spamhaus disponibile all'indirizzo https://www.spamhaus.org/lookup/ per determinare se vi sono domini presenti nella blocklist dei domini di Spamhaus.

- Attieniti alle seguenti best practice di settore durante la progettazione delle e-mail.

Non si tratta di un elenco esaustivo, ma dovrebbe aiutarti a identificare alcuni dei fattori più comuni che potrebbero indurre a contrassegnare le tue e-mail.

Spamhaus Domain Blocklist non è affiliato con Amazon SES o AWS. Non forniamo alcuna garanzia circa l'accuratezza dei domini in questo elenco. Gli strumenti Spamhaus Domain Blocklist e Domain Lookup sono di proprietà di Spamhaus Project, che ne cura anche la gestione e la manutenzione.

Account in fase di verifica o capacità del tuo account di inviare e-mail sospesa

Quando hai effettuato le modifiche che ritieni possano risolvere il problema, accedi alla console AWS e vai nel Centro assistenza. Rispondi al caso che abbiamo aperto per tuo conto. Fornisci informazioni dettagliate sulle operazioni che hai effettuato per risolvere il problema e descrivi in che modo tali interventi potranno evitare che il problema si ripeta in futuro. Se riteniamo che le modifiche apportate possano risolvere in modo appropriato il problema, annulliamo il periodo di verifica o la sospensione dell'invio del tuo account.

Se rimuoviamo un periodo di verifica o la sospensione dell'invio dal tuo account e osserviamo che lo stesso problema si verifica successivamente, potremmo collocare il tuo account in fase di verifica o sospendere la capacità di inviare ancora e-mail. In casi estremi, oppure se osserviamo ripetutamente il verificarsi dello stesso problema, potremmo sospendere definitivamente la capacità del tuo account di inviare e-mail.

Consulta Domande frequenti sul processo di verifica dell'invio di Amazon SES per ulteriori informazioni su cosa fare se il tuo account è in fase di verifica o se la capacità del tuo account di inviare e-mail è stata sospesa.

Notifica di fornitori di mailbox

Questa sezione contiene ulteriori informazioni sulle notifiche dei fornitori di mailbox bloccati mostrate nella pagina dei parametri di reputazione Amazon SES.

Perché hai ricevuto questa notifica

Un importante fornitore di mailbox ci ha segnalato che e-mail non richieste o dannose vengono inviate da un indirizzo o un dominio associato al tuo account Amazon SES.

Non possiamo divulgare l'identità dell'organizzazione che ha emesso il report. Inoltre, non abbiamo informazioni sui fattori specifici che hanno indotto il fornitore di mailbox a emettere il report. Di

solito, i fornitori di mailbox prendono questa decisione in base al feedback dei clienti, ai parametri di coinvolgimento dei clienti, ai tentativi di consegna a indirizzi non validi e a contenuto che viene contrassegnato da filtri antispam. Non si tratta di un elenco esaustivo; altri fattori potrebbero aver indotto il fornitore di mailbox a contrassegnare i tuoi contenuti.

Cosa puoi fare per risolvere il problema

Per risolvere questo problema, devi determinare quali aspetti del tuo programma di invio di e-mail potrebbero aver indotto i fornitori di mailbox a contrassegnare la tua posta come problematica. Devi quindi modificare il programma di invio per risolvere i problemi individuati.

Se il tuo account è in fase di verifica

Alla fine del periodo di verifica, se il fornitore di mailbox continua a identificare le e-mail inviate dal tuo account come problematiche, potremmo sospendere la capacità del tuo account di inviare e-mail finché non risolvi il problema.

Se hai effettuato delle modifiche che ritieni possano risolvere il problema, accedi alla console AWS e vai nel Centro assistenza. Rispondi al caso che abbiamo aperto per tuo conto. Nel tuo messaggio, fornisci i dettagli delle modifiche apportate. Una volta ricevute queste informazioni, estenderemo il periodo di verifica per assicurarci di analizzare solo il numero di notifiche del fornitore di mailbox ricevute dopo che hai implementato le modifiche. Se, al termine di questa estensione del periodo di verifica, il tuo account non viene più segnalato dal fornitore di mailbox come problematico, potremmo rimuovere lo stato di verifica dal tuo account.

Sospensione della capacità del tuo account di inviare e-mail

Puoi chiederci di rivedere tale decisione. Per ulteriori informazioni, consulta Domande frequenti sul processo di verifica dell'invio di Amazon SES.

Quando hai effettuato le modifiche che ritieni possano risolvere il problema, accedi alla console AWS e vai nel Centro assistenza. Rispondi al caso che abbiamo aperto per tuo conto. Includi i dettagli delle azioni intraprese per risolvere il problema, nonché i dettagli dei piani volti ad assicurare che questo problema non si verifichi nuovamente. Dopo aver ricevuto la tua richiesta, esaminiamo le informazioni che hai fornito e modifichiamo lo stato del tuo account, se necessario.

Notifica di feedback dei destinatari

Questa sezione contiene ulteriori informazioni sulle notifiche di feedback dei destinatari mostrate nella pagina dei parametri di reputazione Amazon SES.

Perché hai ricevuto questa notifica

Un importante fornitore di mailbox ha segnalato che un numero elevato di suoi utenti denuncia e-mail non richieste provenienti dal tuo account Amazon SES. Questo tipo di feedback non è visibile nei reclami segnalati direttamente dai fornitori di mailbox e non è incluso nelle notifiche di mancati recapiti e reclami Amazon SES.

Un numero elevato di reclami può avere ripercussioni negative su tutti gli utenti Amazon SES. Per proteggere la tua reputazione e quella degli altri clienti Amazon SES, interveniamo immediatamente quando un account riceve un certo numero di reclami.

Non possiamo fornire un elenco di indirizzi e-mail specifici che segnalano la tua posta come non richiesta. Inoltre, non possiamo divulgare il nome del fornitore di mailbox che ci ha segnalato il problema.

Cosa puoi fare per risolvere il problema

Per risolvere questo problema, devi determinare quali aspetti del tuo programma di invio di e-mail potrebbero indurre i destinatari a presentare reclami per i messaggi che ricevono da te. Dopo aver identificato questi fattori, correggi le pratiche di invio delle e-mail.

Per acquisire nuovi indirizzi, consigliamo di implementare una strategia con doppio consenso esplicito, come descritto in Creazione e gestione degli elenchi, nonché di inviare e-mail solo agli indirizzi che hanno completato il processo di doppio consenso.

Inoltre, dovresti eliminare gli elenchi di indirizzi che non hanno interagito con le tue e-mail di recente. Puoi utilizzare il tracciamento di apertura e clic, come descritto in Monitoraggio delle attività di invio di Amazon SES, per determinare quali utenti visualizzano e interagiscono con il contenuto inviato.

Se il tuo account è in fase di verifica

Alla fine del periodo di verifica, se il fornitore di mailbox continua a segnalare un numero rilevante di reclami diretti in relazione ai messaggi inviati dal tuo account, potremmo sospendere la capacità del tuo account di inviare e-mail finché non risolvi il problema.

Se hai effettuato delle modifiche che ritieni possano risolvere il problema, accedi alla console AWS e vai nel Centro assistenza. Rispondi al caso che abbiamo aperto per tuo conto. Nel tuo messaggio, fornisci i dettagli delle modifiche apportate. Una volta ricevute queste informazioni, estenderemo il periodo di verifica per assicurarci di analizzare solo il numero di reclami del fornitore di mailbox

ricevuti dopo che hai implementato le modifiche. Al termine di questa estensione del periodo di verifica, se il numero di reclami del fornitore di mailbox risulta ridotto o eliminato, potremmo rimuovere lo stato di verifica dal tuo account.

Sospensione della capacità del tuo account di inviare e-mail

Puoi chiederci di rivedere tale decisione. Per ulteriori informazioni, consulta Domande frequenti sul processo di verifica dell'invio di Amazon SES.

Quando hai effettuato le modifiche che ritieni possano risolvere il problema, accedi alla console AWS e vai nel Centro assistenza. Rispondi al caso che abbiamo aperto per tuo conto. Includi i dettagli delle azioni intraprese per risolvere il problema, nonché i dettagli dei piani volti ad assicurare che questo problema non si verifichi nuovamente. Dopo aver ricevuto la tua richiesta, esaminiamo le informazioni che hai fornito e modifichiamo lo stato del tuo account, se necessario.

Notifica di account correlato

Questa sezione contiene ulteriori informazioni sulle notifiche di account correlato mostrate nella pagina dei parametri di reputazione Amazon SES.

Perché hai ricevuto questa notifica

Abbiamo rilevato gravi problemi relativi a e-mail inviate da un altro account Amazon SES. Riteniamo che l'account problematico sia correlato al tuo account Account AWS, perciò siamo intervenuti per evitare problemi simili.

Cosa puoi fare per risolvere il problema

Quando sospendiamo la capacità di un account di inviare e-mail, inviamo sempre informazioni sui motivi della sospensione dell'invio al proprietario dell'account. Consulta le e-mail che abbiamo inviato al proprietario dell'account per ulteriori informazioni.

Dovresti per prima cosa risolvere i problemi relativi all'account. Dopo aver effettuato delle modifiche che ritieni possano risolvere il problema, accedi alla console AWS e vai nel Centro assistenza. Rispondi al caso che abbiamo aperto per tuo conto. Fornisci informazioni dettagliate sulle operazioni che hai effettuato per risolvere il problema e descrivi in che modo tali interventi potranno evitare che il problema si ripeta in futuro. Se riteniamo che le modifiche apportate possano risolvere in modo appropriato il problema, annulliamo il periodo di verifica o la sospensione dell'invio del tuo account.

Notifica di spamtrap

Questa sezione contiene ulteriori informazioni sulle notifiche di trappole per spam mostrate nella pagina dei parametri di reputazione Amazon SES.

Perché hai ricevuto questa notifica

Un'organizzazione antispam di terza parte ci ha segnalato che i loro indirizzi di trappole per spam hanno recentemente ricevuto e-mail da un indirizzo o un dominio verificato associato al tuo account Amazon SES.

Uno spamtrap, o trappola per spam, è un indirizzo e-mail inattivo che viene utilizzato esclusivamente per attrarre e-mail non richieste (spam). Un numero elevato di report di trappole per spam può avere ripercussioni negative su tutti gli utenti Amazon SES. Per proteggere la tua reputazione e quella degli altri clienti Amazon SES, interveniamo immediatamente quando un account invia un certo volume di e-mail a indirizzi spamtrap.

Cosa puoi fare per risolvere il problema

Non possiamo rivelare gli indirizzi e-mail spamtrap che hanno ricevuto le e-mail. Questi indirizzi sono rigidamente protetti dalle organizzazioni proprietarie perché, una volta resi noti, diventano inutili.

L'invio di e-mail a indirizzi spamtrap in genere indica un problema nel modo in cui acquisisci gli indirizzi e-mail dei tuoi clienti. Ad esempio, elenchi acquistati di indirizzi e-mail possono contenere indirizzi spamtrap, che è il motivo per cui l'invio a elenchi acquistati o noleggiati è vietato dalle condizioni del servizio Amazon SES. Per acquisire nuovi indirizzi, consigliamo di implementare una strategia con doppio consenso esplicito, come descritto in Creazione e gestione degli elenchi, nonché di inviare e-mail solo agli indirizzi che hanno completato il processo di doppio consenso.

Inoltre, dovresti eliminare gli elenchi di indirizzi che non hanno interagito con le tue e-mail di recente. Puoi utilizzare il tracciamento di apertura e clic, come descritto in Monitoraggio delle attività di invio di Amazon SES, per determinare quali utenti visualizzano e interagiscono con il contenuto inviato.

Se il tuo account è in fase di verifica

Alla fine del periodo di verifica, se i messaggi vengono ancora inviati verso indirizzi spamtrap dal tuo account, potremmo sospendere la capacità del tuo account di inviare e-mail finché non risolvi il problema.

Se hai effettuato delle modifiche che ritieni possano risolvere il problema, accedi alla console AWS e vai nel Centro assistenza. Rispondi al caso che abbiamo aperto per tuo conto. Nel tuo messaggio,

fornisci i dettagli delle modifiche apportate. Una volta ricevute queste informazioni, estenderemo il periodo di verifica per assicurarci di analizzare solo il numero di report di spamtrap ricevuti dopo che hai implementato le modifiche. Se, al termine di questa estensione del periodo di verifica, il numero di report di spamtrap risulta ridotto o eliminato, potremmo rimuovere lo stato di verifica dal tuo account.

Sospensione della capacità del tuo account di inviare e-mail

Puoi chiederci di rivedere tale decisione. Per ulteriori informazioni, consulta Domande frequenti sul processo di verifica dell'invio di Amazon SES.

Quando hai effettuato le modifiche che ritieni possano risolvere il problema, accedi alla console AWS e vai nel Centro assistenza. Rispondi al caso che abbiamo aperto per tuo conto. Includi i dettagli delle azioni intraprese per risolvere il problema, nonché i dettagli dei piani volti ad assicurare che questo problema non si verifichi nuovamente. Dopo aver ricevuto la tua richiesta, esaminiamo le informazioni che hai fornito e modifichiamo lo stato del tuo account, se necessario.

Notifica di sito vulnerabile

Questa sezione contiene ulteriori informazioni sulle notifiche di sito vulnerabile mostrate nella pagina dei parametri di reputazione Amazon SES.

Perché hai ricevuto questa notifica

Una revisione completa ha rilevato che dal tuo account vengono inviati messaggi che riteniamo tu non intenda inviare. È molto probabile che questi messaggi vengano contrassegnati come spam dai fornitori di mailbox e dai destinatari.

Molto spesso in queste situazioni una terza parte sta utilizzando illecitamente una caratteristica del tuo sito Web per inviare e-mail indesiderate. Ad esempio, se il tuo sito Web contiene un'opzione "invia un'e-mail a un amico", "contattaci", "invita un amico" o simile, una terza parte può sfruttare questa caratteristica per inviare e-mail non richieste.

Cosa puoi fare per risolvere il problema

In primo luogo, identifica le caratteristiche del tuo sito Web o delle tue applicazioni che potrebbero consentire a terze parti di inviare e-mail utilizzando Amazon SES senza che tu ne sia consapevole. Nella pratica del Centro assistenza è possibile richiedere un esempio dei messaggi che riteniamo siano stati inviati in questo modo.

Quindi, modifica l'applicazione o il sito Web per evitare l'invio non richiesto. Ad esempio, aggiungi un CAPTCHA, limita la velocità a cui le e-mail possono essere inviate, togli agli utenti la possibilità

di inviare contenuti personalizzati, richiedi agli utenti di effettuare l'accesso per inviare e-mail e impedisci all'applicazione di generare più notifiche simultanee.

Account in fase di verifica o capacità del tuo account di inviare e-mail sospesa

Quando hai effettuato le modifiche che ritieni possano risolvere il problema, accedi alla console AWS e vai nel Centro assistenza. Rispondi al caso che abbiamo aperto per tuo conto. Includi i dettagli delle azioni intraprese per risolvere il problema, nonché i dettagli dei piani volti ad assicurare che questo problema non si verifichi nuovamente. Dopo aver ricevuto la tua richiesta, esaminiamo le informazioni che hai fornito e modifichiamo lo stato del tuo account, se necessario.

Se rimuoviamo un periodo di verifica o la sospensione dell'invio dal tuo account e osserviamo che lo stesso problema si verifica successivamente, potremmo collocare il tuo account in fase di verifica o sospendere la capacità di inviare ancora e-mail. In casi estremi, oppure se osserviamo ripetutamente il verificarsi dello stesso problema, potremmo sospendere definitivamente la capacità del tuo account di inviare e-mail.

Consulta Domande frequenti sul processo di verifica dell'invio di Amazon SES per ulteriori informazioni su cosa fare se il tuo account è in fase di verifica o se la capacità del tuo account di inviare e-mail è stata sospesa.

Notifica contro le credenziali compromesse

Questa sezione contiene ulteriori informazioni sulle notifiche del sito di credenziali compromesso mostrate nella pagina delle metriche di reputazione Amazon SES.

Perché hai ricevuto questa notifica

Una revisione completa ha rilevato che dal tuo account vengono inviati messaggi che riteniamo tu non intenda inviare. È molto probabile che questi messaggi vengano contrassegnati come spam dai fornitori di mailbox e dai destinatari.

Alcune cause comuni sono le chiavi di accesso IAM compromesse, le password SMTP compromesse o altre vulnerabilità di sicurezza.

Cosa puoi fare per risolvere il problema

È necessario eseguire una revisione completa della sicurezza dei meccanismi di utilizzo di SES. Assicurarsi di aver ruotato tutte le password SMTP o applicabili e di aver rimosso eventuali utenti o risorse non autorizzati dall'account. Assicurati di non archiviare informazioni sensibili come password o chiavi di accesso su siti Web o repository di terze parti. È consigliabile non utilizzare le chiavi di

accesso IAM per gli utenti e mai per l'utente root. Se sono ancora utilizzate, è opportuno eseguirne la migrazione a meccanismi che forniscono credenziali temporanee come la creazione di un utente in AWS IAM Identity Center.

Account in fase di verifica o capacità del tuo account di inviare e-mail sospesa

Quando hai effettuato le modifiche che ritieni possano risolvere il problema, accedi alla console AWS e vai nel Centro assistenza. Rispondi al caso che abbiamo aperto per tuo conto. Includi i dettagli delle azioni intraprese per risolvere il problema, nonché i dettagli dei piani volti ad assicurare che questo problema non si verifichi nuovamente. Dopo aver ricevuto la tua richiesta, esaminiamo le informazioni che hai fornito e modifichiamo lo stato del tuo account, se necessario.

Se rimuoviamo un periodo di verifica o la sospensione dell'invio dal tuo account e osserviamo che lo stesso problema si verifica successivamente, potremmo collocare il tuo account in fase di verifica o sospendere la capacità di inviare ancora e-mail. In casi estremi, oppure se osserviamo ripetutamente il verificarsi dello stesso problema, potremmo sospendere definitivamente la capacità del tuo account di inviare e-mail.

Consulta Domande frequenti sul processo di verifica dell'invio di Amazon SES per ulteriori informazioni su cosa fare se il tuo account è in fase di verifica o se la capacità del tuo account di inviare e-mail è stata sospesa.

Notifica di altro tipo

Questa sezione contiene ulteriori informazioni sulle notifiche di altro tipo mostrate nella pagina dei parametri di reputazione Amazon SES.

Perché hai ricevuto questa notifica

Una revisione automatica o umana ha individuato problemi che non sono elencati nelle sezioni precedenti di questo documento.

Cosa puoi fare per risolvere il problema

Per ulteriori informazioni sul problema specifico, fare riferimento alla pratica nel Centro assistenza che abbiamo aperto per tuo conto. Per accedere al Centro assistenza, accedi all'AWS Management Console e scegli Support Center (Centro assistenza). Nella risposta alla pratica, descrivi le modifiche che hai implementato. In base alla situazione specifica e alla natura dei problemi che abbiamo rilevato, potremmo terminare il periodo di verifica o ripristinare la capacità del tuo account di inviare e-mail.

Creazione di allarmi di monitoraggio della reputazione tramite CloudWatch

Amazon SES pubblica automaticamente una serie di parametri relativi alla reputazione su Amazon CloudWatch. Puoi utilizzare questi parametri per creare allarmi che inviano una notifica quando le percentuali di mancati recapiti o reclami raggiungono livelli che potrebbero influire sulla capacità dell'account di inviare e-mail.

> **Note**
>
> La parte relativa a CloudWatch nelle procedure di questa sezione ha lo scopo di presentare i passaggi fondamentali per impostare un allarme CloudWatch per monitorare la reputazione del mittente SES. Non esplora le configurazioni avanzate relative alle impostazioni facoltative per gli allarmi CloudWatch. Per informazioni complete sulla configurazione degli allarmi CloudWatch, consulta Utilizzo degli allarmi di Amazon CloudWatch nella Guida per l'utente di Amazon CloudWatch.

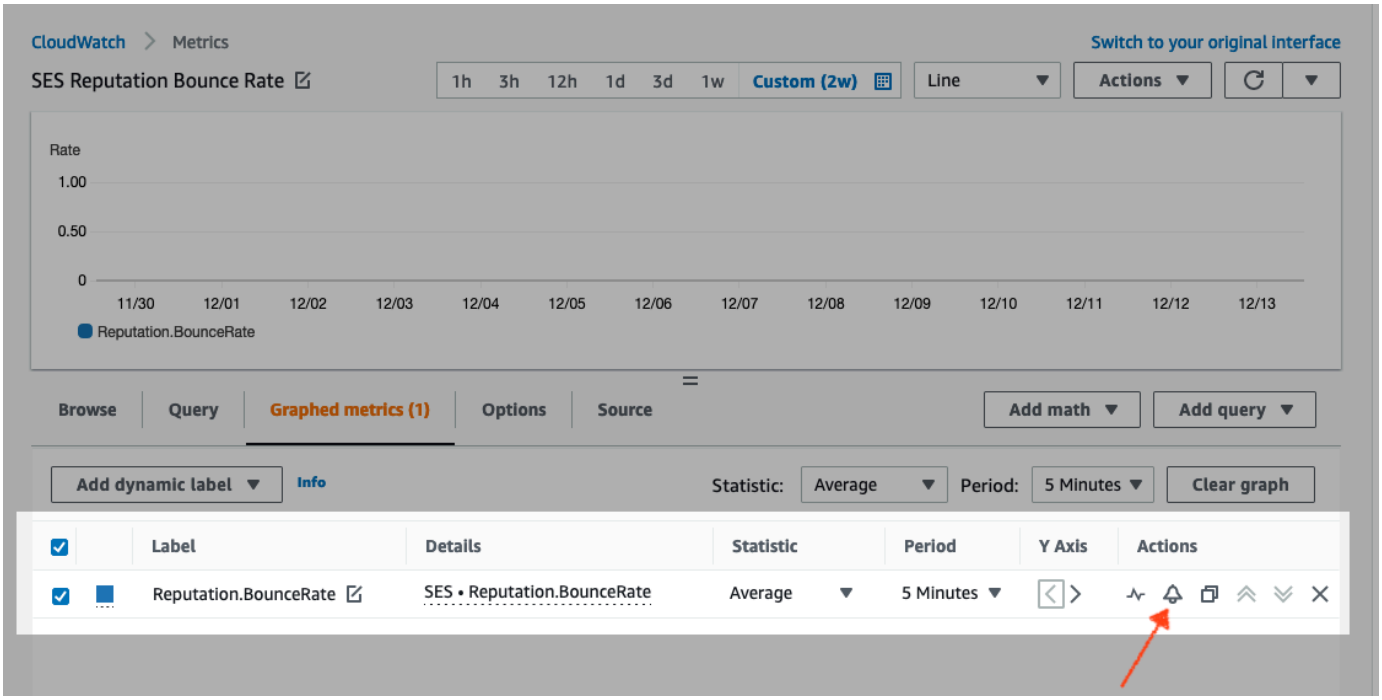
Prerequisiti

- Crea un nuovo argomento Amazon SNS, quindi esegui la sottoscrizione tramite l'endpoint che preferisci (ad esempio e-mail o SMS). Per ulteriori informazioni, consulta Creare un argomento Amazon SNS e Iscrizione a un argomento Amazon SNS nella Guida per gli sviluppatori di Amazon Simple Notification Service.
- Se non hai mai inviato un'e-mail nella regione corrente, potresti non visualizzare lo spazio dei nomi SES. Per assicurarti di disporre delle metriche, invia un'e-mail di prova al simulatore di mailbox.

Creazione di un allarme CloudWatch per monitorare la reputazione di invio

1. Accedi alla AWS Management Console e apri la console Amazon SES all'indirizzo https://console.aws.amazon.com/ses/.
2. Nel pannello di navigazione sul lato sinistro dello schermo, scegli Reputation metrics (Parametri di reputazione).
3. Nella pagina Parametri di reputazione sotto la scheda A livello di account, nei riquadri Percentuale di mancati recapiti o Percentuale di reclami, scegli Visualizza in CloudWatch: si aprirà la console CloudWatch con il parametro scelto.

4. Nella scheda Graphed metrics (Parametri dei grafici), sulla riga del parametro scelto, per questo esempio, Reputation.BounceRate, scegli l'icona del campanello di allarme nella colonna Actions (Operazioni) (vedi immagine sotto): si aprirà la pagina Specify metric and conditions (Specificare parametri e condizioni).



5. Scorri fino al riquadro Conditions (Condizioni) e scegli Static (Statico) nel campo Threshold type (Tipo di soglia).

   a. Nel campo Whenever ***`metric`*** is...(Ogni volta che il parametro è...), scegli Greater/Equal (Maggiore/Uguale a).

   b. Nel campo than... (di...), specifica il valore che comporta l'attivazione di un allarme da parte di CloudWatch.

      - Se stai creando un allarme per monitorare la percentuale di mancati recapiti, tieni presente che Amazon SES consiglia una percentuale inferiore al 5%. Se la percentuale di mancati recapiti per il tuo account è superiore al 10%, è possibile che venga sospesa automaticamente la capacità dell'account di inviare e-mail. Per questo motivo, devi configurare CloudWatch in modo che invii una notifica quando la percentuale di mancati recapiti del tuo account è maggiore o uguale a 0,05 (5%).
      - Se stai creando un allarme per monitorare la percentuale di reclami, tieni presente che Amazon SES consiglia una percentuale inferiore allo 0,1%. Se la percentuale di reclami per il tuo account è superiore allo 0,5%, è possibile che venga sospesa automaticamente la capacità dell'account di inviare e-mail. Per questo motivo, devi configurare CloudWatch

in modo che invii una notifica quando la percentuale di reclami del tuo account è maggiore o uguale a 0,001 (0,1%).

c. Espandi Additional configuration (Configurazione aggiuntiva), scegli Treat missing data as ignore (maintain the alarm state) (Tratta dati mancanti come ignorati mantenendo lo stato dell'allarme) nel campo Missing data treatment (Trattamento dati mancanti).

d. Seleziona Successivo.

6. Nel riquadro Configure actions (Configura operazioni), scegli In alarm (In allarme) nel campo Alarm state trigger (Attivazione dello stato di allarme).

a. Scegli Select an existing SNS topic (Seleziona un argomento SNS esistente) nel campo Select an SNS topic (Seleziona un argomento SNS).

b. Nella casella di ricerca Send a notification to... (Invia notifica a...), scegli l'argomento che hai creato e a cui hai eseguito la sottoscrizione nei prerequisiti.

c. Seleziona Successivo.

7. Nel riquadro Add name and description (Aggiungi nome e descrizione), immetti un nome e una descrizione per l'allarme e scegli Next (Successivo).

8. Nel riquadro Preview and create (Visualizza in anteprima e crea), conferma le impostazioni e, se ti soddisfano, scegli Create alarm (Crea allarme). Se c'è qualcosa che vorresti modificare, seleziona il pulsante Previous (Precedente) per ogni sezione a cui desideri tornare e apportare modifiche.

Parametri SNDS per gli indirizzi IP dedicati

È possibile visualizzare i dati SNDS (Smart Network Data Services) per gli indirizzi IP dedicati noleggiati in ogni Regione AWS in cui si utilizza Amazon SES. Questi dati SNDS sono disponibili tramite la console Amazon CloudWatch.

SNDS è un programma di Outlook che consente ai proprietari di IP di aiutare a prevenire lo spam all'interno del loro spazio IP. Amazon SES fornisce questi dati importanti per coloro che affittano IP dedicati. I dati SNDS forniscono informazioni dettagliate sul comportamento di invio della posta IP e richiamano le aree di preoccupazione per la reputazione del mittente.

> **Note**
>
> Quando si fa riferimento a Outlook, questo copre tutti i domini che tracciano. Ad esempio, questo può coprire Hotmail.com, Outlook.com e Live.com.

Visualizzazione dei dati SNDS per gli indirizzi IP dedicati

1. Accedi alla console Amazon CloudWatch all'indirizzo https://console.aws.amazon.com/cloudwatch/.
2. Nel pannello di navigazione, scegli Metrics (Parametri), quindi scegli All metrics (Tutti i parametri).

   (Vengono fornite istruzioni per la nuova interfaccia della console CloudWatch.)
3. Nella scheda Browse (Sfoglia) nel container Metrics (Parametri), seleziona la Regione AWS, quindi scegli SES.
4. Scegli IP Metrics (Parametri IP) per visualizzare tutti i tuoi IP dedicati tracciati da SNDS.

   (Nota: se non ci sono indirizzi IP dedicati associati al tuo account nella Regione selezionata, IP Metrics (Parametri IP) non viene visualizzato nella console CloudWatch.)
5. Visualizza tutti gli IP dedicati tracciati da SNDS in questo elenco o seleziona un singolo indirizzo IP per visualizzarne solo i relativi parametri.

I seguenti parametri sono forniti per ogni indirizzo IP dedicato e definito da Outlook. Per ulteriori informazioni, consulta le domande frequenti per SNDS di Outlook.

> **Note**
>
> Questi parametri rappresentano un periodo di attività che fornisce dati aggiornati una volta al giorno. I parametri presentano anche un timestamp corrispondente, che riflette un periodo di tempo di 24 ore

- SNDS.RCPTCommands: indica il numero di comandi RCPT percepiti da SNDS per l'indirizzo IP specifico durante il periodo di attività. I comandi RCPT fanno parte del protocollo SMTP utilizzato per inviare l'e-mail, che specifica l'indirizzo del destinatario a cui si sta tentando di recapitare il messaggio.

- SNDS.DATACommands: indica il numero di comandi DATA percepiti da SNDS per l'indirizzo IP specifico durante il periodo di attività. I comandi DATA fanno parte del protocollo SMTP utilizzato per inviare l'e-mail, in particolare quella parte che trasmette effettivamente il messaggio ai destinatari previsti precedentemente stabiliti.
- SNDS.MessageRecipients: indica il numero di destinatari dei messaggi percepiti da SNDS per l'indirizzo IP specifico durante il periodo di attività.
- SNDS.SpamRate: visualizza i risultati aggregati del filtro antispam applicato a tutti i messaggi inviati dall'indirizzo IP durante il periodo di attività specificato.
  - Uno SpamRate pari a 0 indica che l'indirizzo IP ha meno del 10% di spam.
  - Uno SpamRate pari a 0,5 significa che dall'indirizzo IP viene generato tra il 10% e il 90% di spam.
  - Uno SpamRate pari a 1 significa che dall'indirizzo IP viene generato almeno il 90% di spam.
- SNDS.ComplaintRate: corrisponde alla frazione di tempo in cui un utente di Outlook invia un reclamo per un messaggio ricevuto dall'IP durante il periodo di attività.
  - Un ComplaintRate pari a 1 significa un tasso di reclamo del 100%.
  - Un ComplaintRate pari a 0,05 significherebbe, ad esempio, un tasso di reclamo del 5%.
  - Un ComplaintRate pari a 0 indica che il tasso è inferiore allo 0,1%.
- SNDS.TrapHits: mostra il numero di messaggi inviati agli "account trap". Gli account trap sono account gestiti da Outlook che non richiedono posta elettronica. Pertanto, qualsiasi messaggio inviato agli account trap è molto probabile che sia spam.

Suggerimenti sulla risoluzione dei problemi

D1. Perché i dati non si popolano ogni giorno? È possibile applicare uno dei seguenti scenari:

- I dati SNDS dipendono dal programma SNDS di Outlook.
- Esiste una soglia minima di messaggi di posta elettronica che SNDS deve ricevere per calcolare un valore. I dati potrebbero non essere disponibili nei momenti in cui il volume di posta elettronica su un IP risultava basso.

D2. Perché i parametri SNDS.SpamRate e SNDS.ComplaintRate cambiano e cosa devo fare se il tasso assume un valore pari a 1?

Si tratta di un indicatore che qualcosa nel comportamento di invio ha attivato una risposta negativa dal programma SNDS di Outlook. In questo caso, si desidera controllare altri fornitori di servizi

Internet (ISP) e i numeri di coinvolgimento per assicurarsi che non si tratti di un problema globale. Se si tratta di un problema globale, è possibile che si verifichino problemi con più ISP, che suggeriscono un problema di elenco, contenuto, distribuzione o autorizzazioni. Se è specifico di Outlook, consulta come inviare al meglio a Outlook.

D3. Quali azioni intraprenderà AWS Support se il mio SNDS.SpamRate passa da 0 (o 0,5) a 1?

AWS non ha alcun controllo su SNDS e quindi non ha alcuna influenza su SNDS. Tutte le richieste di mitigazione devono essere archiviate direttamente con Outlook tramite il loro nuovo modulo di richiesta di supporto.

Sospensione automatica dell'invio di e-mail

Per proteggere la reputazione del mittente, puoi sospendere temporaneamente l'invio dei messaggi inviati tramite specifici set di configurazione o di tutti i messaggi inviati dal tuo account Amazon SES in una specifica Regione AWS.

Utilizzando Amazon CloudWatch e Lambda, puoi creare una soluzione in grado di sospendere automaticamente l'invio delle e-mail quando i parametri di reputazione (ad esempio la percentuale di mancati recapiti o di reclami) superano determinate soglie. Questo argomento descrive le procedure per la configurazione di questa soluzione.

Argomenti in questa sezione:

- Sospensione automatica dell'invio di e-mail per l'intero account Amazon SES
- Sospensione automatica dell'invio di e-mail per un set di configurazione

Sospensione automatica dell'invio di e-mail per l'intero account Amazon SES

In questa sezione viene illustrata la procedura per configurare Amazon SES, Amazon SNS, Amazon CloudWatch e AWS Lambda in modo che sospendano automaticamente l'invio di e-mail per l'account Amazon SES in una sola Regione AWS. Se invii e-mail da diverse Regioni, ripeti le procedure di questa sezione per ogni Regione in cui desideri implementare questa soluzione.

Argomenti in questa sezione:

- Fase 1: creazione di un ruolo IAM

- Fase 2: creazione della funzione Lambda
- Fase 3: riabilitazione dell'invio di e-mail per l'account
- Fase 4: creazione di un argomento Amazon SNS e sottoscrizione
- Fase 5: creazione di un allarme CloudWatch
- Fase 6: verifica della soluzione

Fase 1: creazione di un ruolo IAM

La prima fase per la configurazione della sospensione automatica dell'invio di e-mail consiste nel creare un ruolo IAM in grado di eseguire l'operazione API `UpdateAccountSendingEnabled`.

Creazione del ruolo IAM

1. Apri la console IAM all'indirizzo https://console.aws.amazon.com/iam/.
2. Nel pannello di navigazione, seleziona Roles (Ruoli).
3. Selezionare Create role (Crea ruolo).
4. Nella pagina Select trusted entity (Seleziona entità attendibile), scegli AWSservice (Servizio) per Trusted entity type (tipo Entità attendibile).
5. In Use case (Caso d'uso), scegli Lambda e quindi scegli Next (Successivo).
6. Nella pagina Add permissions (Aggiungi autorizzazioni), scegli le policy seguenti:

   - AWSLambdaBasicExecutionRole
   - AmazonSESFullAccess

   > **Tip**
   >
   > Utilizzare la casella di ricerca in Policy di autorizzazione per individuare rapidamente queste policy, ma si noti che dopo aver cercato e selezionato la prima policy, è necessario scegliere Clear filters (Cancella filtri) prima di cercare e selezionare la seconda policy.

   Quindi scegli Next (Successivo).
7. Nella pagina Name, review, and create (Assegna nome, rivedi e crea), in Dettagli ruolo, inserisci un nome significativo per la policy nel campo Nome ruolo.

8. Verificare che le due policy selezionate siano elencate nella tabella Riepilogo della policy di autorizzazione, quindi scegliere Create role (Crea ruolo).

Fase 2: creazione della funzione Lambda

Dopo aver creato un ruolo IAM, puoi creare la funzione Lambda per la sospensione dell'invio di e-mail per il tuo account.

Creazione della funzione Lambda

1. Apri la console AWS Lambda all'indirizzo https://console.aws.amazon.com/lambda/.
2. Usa il selettore della Regione per scegliere la Regione in cui desideri distribuire questa funzione Lambda.

   > **Note**
   >
   > Questa funzione sospende l'invio di e-mail solo per la regione AWS selezionata in questa fase. Se invii e-mail da più Regioni, ripeti le procedure di questa sezione per ogni Regione in cui desideri che venga sospeso automaticamente l'invio di e-mail.

3. Seleziona Create function (Crea funzione).
4. In Create function (Crea funzione), scegli Author from scratch (Crea da zero).
5. In Informazioni di base eseguire queste operazioni:

   - Per Nome digita un nome per la funzione Lambda.
   - Per Tempo di esecuzione, scegli Node.js 14 (o la versione attualmente disponibile nell'elenco selezionato).
   - Per Architettura, mantieni il valore predefinito preselezionato, x86_64.
   - In autorizzazioni, espandi Change default execution role (Modifica ruolo di esecuzione predefinito) e scegli Use an existing role (Usa un ruolo esistente).
   - Fai clic all'interno dell'elenco Ruolo esistente e scegli il ruolo IAM creato in the section called "Fase 1: creazione di un ruolo IAM".

   Quindi, seleziona Crea funzione.
6. In Fonte funzione, nell'editor di codice, incolla il codice seguente:

```
'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);
        }
    });
};
```

Scegliere quindi Deploy (Distribuisci).

7. Scegli Test (Esegui test). Se viene visualizzata la finestra Configure test event (Configura evento test), digita un nome nel campo Nome evento), quindi scegli Create (Crea).
8. Espandi la casella Test e seleziona il nome dell'evento appena creato e quindi scegli Test.
9. Apparirà la scheda Risultati dell'esecuzione, appena sotto e a destra; assicurati che venga visualizzato `Status: Succeeded`. Se l'esecuzione della funzione non è riuscita, procedi nel seguente modo:

   - Verifica che il ruolo IAM creato in the section called “Fase 1: creazione di un ruolo IAM” contenga le policy corrette.
   - Verifica che il codice nella funzione Lambda non contenga errori. L'editor di codice Lambda evidenzia automaticamente gli errori di sintassi e altri potenziali problemi.

Fase 3: riabilitazione dell'invio di e-mail per l'account

Un effetto secondario del test della funzione Lambda in the section called “Fase 2: creazione della funzione Lambda” è la sospensione dell'invio di e-mail per l'account Amazon SES. Nella maggior parte dei casi, è preferibile non sospendere l'invio per l'account finché non viene attivato l'allarme CloudWatch.

Le procedure in questa sezione consentono di riabilitare l'invio di e-mail per l'account Amazon SES. Per completare questa procedura, è necessario installare e configurare AWS Command Line Interface. Per ulteriori informazioni, consultare la Guida per l'utente di AWS Command Line Interface.

Riabilitazione dell'invio di e-mail

1. Nella riga di comando, digita il comando seguente per riabilitare l'invio di e-mail per tuo account. Sostituisci *sending_region* con il nome della regione in cui desideri abilitare nuovamente l'invio di e-mail.

   ```
   aws ses update-account-sending-enabled --enabled --region sending_region
   ```

2. Nella riga di comando, digita il comando seguente per controllare lo stato dell'invio di e-mail per il tuo account:

   ```
   aws ses get-account-sending-enabled --region sending_region
   ```

   Se viene visualizzato l'output seguente, la riabilitazione dell'invio di e-mail per il tuo account è riuscita:

   ```
   {
       "Enabled": true
   }
   ```

Fase 4: creazione di un argomento Amazon SNS e sottoscrizione

Affinché CloudWatch esegua la tua funzione Lambda quando viene attivato un allarme, è prima necessario creare un argomento Amazon SNS e sottoscrivere la funzione Lambda per l'argomento.

Per creare un argomento Amazon SNS e sottoscrivere la funzione Lambda all'argomento

1. Apri la console Amazon SNS all'indirizzo https://console.aws.amazon.com/sns/v3/home.

2. Crea un argomento seguendo i passaggi della Guida per gli sviluppatori di Amazon Simple Notification Service.

   - In Type (Tipo), deve essere selezionata l'opzione Standard (non FIFO).

3. Effettua la sottoscrizione all'argomento seguendo i passaggi della Guida per gli sviluppatori di Amazon Simple Notification Service.

   a. Per Protocol (Protocollo) scegliere AWS Lambda.

   b. Per Endpoint scegli la funzione Lambda creata in the section called “Fase 2: creazione della funzione Lambda”.

Fase 5: creazione di un allarme CloudWatch

In questa sezione sono incluse le procedure per la creazione di un allarme in CloudWatch che viene attivato quando un parametro raggiunge una determinata soglia. Quando l'allarme viene attivato, recapita una notifica all'argomento Amazon SNS creato in the section called “Fase 4: creazione di un argomento Amazon SNS e sottoscrizione”, che quindi esegue la funzione Lambda creata in the section called “Fase 2: creazione della funzione Lambda”.

Creazione di un allarme CloudWatch

1. Apri la console CloudWatch all'indirizzo https://console.aws.amazon.com/cloudwatch/.
2. Usa il selettore della Regione per scegliere la Regione in cui desideri che l'invio di e-mail venga sospeso automaticamente.
3. Nel pannello di navigazione, seleziona Alarms (Allarmi).
4. Scegli Create Alarm (Crea allarme).
5. Nella finestra Create Alarm (Crea allarme), in SES Metrics (Parametri SES), scegli Account Metrics (Parametri account).
6. In Metric Name (Nome parametro) scegli una delle opzioni seguenti:

   - Reputation.BounceRate: scegli questo parametro se desideri sospendere l'invio di e-mail per il tuo account quando la frequenza globale di mancato recapito permanente per l'account supera una soglia definita.
   - Reputation.ComplaintRate: scegli questo parametro se desideri sospendere l'invio di e-mail per il tuo account quando la frequenza globale di reclami per l'account supera una soglia definita.

Seleziona Successivo.

7. Completa questa procedura:

   - In Alarm Threshold (Soglia allarme) digita un nome per l'allarme in Name (Nome).
   - In Whenever: Reputation.BounceRate (Ogni volta che: Reputation.BounceRate) o Whenever: Reputation.ComplaintRate (Ogni volta che: Reputation.ComplaintRate), specifica la soglia che causa l'attivazione dell'allarme.

     > **Note**
     >
     > Il tuo account viene messo automaticamente in fase di verifica se la frequenza dei mancati recapiti supera il 10% o se la frequenza dei reclami supera lo 0,5%. Quando specifichi una percentuale di mancati recapiti o reclami che comporta l'attivazione dell'allarme CloudWatch, ti consigliamo di usare valori decisamente inferiori a queste percentuali, per evitare che l'account venga messo in fase di verifica.

   - In Actions (Operazioni), in Whenever this alarm (Ogni volta che questo allarme), scegli State is ALARM (Lo stato è ALLARME). Per Send notification to (Invia notifica a) scegli l'argomento Amazon SNS creato in the section called “Fase 4: creazione di un argomento Amazon SNS e sottoscrizione”.

   Scegli Create Alarm (Crea allarme).

Fase 6: verifica della soluzione

A questo punto, puoi testare l'allarme per verificare che esegua la funzione Lambda quando passa nello stato `ALARM`. Puoi usare l'operazione API `SetAlarmState` per modificare temporaneamente lo stato dell'allarme.

Le procedure di questa sezione sono facoltative, ma ti consigliamo di completarle per assicurarti che l'intera soluzione sia configurata correttamente.

1. Nella riga di comando, digita il comando seguente per controllare lo stato dell'invio di e-mail per il tuo account. Sostituisci *`region`* con il nome della regione.

   ```
   aws ses get-account-sending-enabled --region region
   ```

Se l'invio è abilitato per il tuo account, verrà visualizzato l'output seguente:

```
{
    "Enabled": true
}
```

2. Nella riga di comando, digita il comando seguente per modificare temporaneamente lo stato di allarme in ALARM: aws cloudwatch set-alarm-state --alarm-name ***MyAlarm*** --state-value ALARM --state-reason "Testing execution of Lambda function" --region ***region***

   Nel comando precedente, sostituisci *MyAlarm* con il nome dell'allarme creato in the section called “Fase 5: creazione di un allarme CloudWatch” e sostituisci *region* con la regione in cui desideri sospendere automaticamente l'invio di e-mail.

   > **Note**
   >
   > Quando esegui questo comando, lo stato dell'allarme passa da OK a ALARM e torna a OK entro pochi secondi. Puoi vedere queste modifiche dello stato nella scheda History (Cronologia) dell'allarme nella console CloudWatch oppure con l'operazione DescribeAlarmHistory.

3. Nella riga di comando, digita il comando seguente per controllare lo stato dell'invio di e-mail per il tuo account.

   ```
   aws ses get-account-sending-enabled --region region
   ```

   Se la funzione Lambda viene eseguita correttamente, viene visualizzato il seguente output:

   ```
   {
       "Enabled": false
   }
   ```

4. Completa le fasi in the section called “Fase 3: riabilitazione dell'invio di e-mail per l'account” per riabilitare l'invio di e-mail per il tuo account.

Sospensione automatica dell'invio di e-mail per un set di configurazione

È possibile configurare Amazon SES per esportare i parametri di reputazione specifici delle e-mail inviate usando un determinato set di configurazione in Amazon CloudWatch. È quindi possibile usare questi parametri per creare allarmi CloudWatch specifici per questi set di configurazione. Quando questi allarmi superano determinate soglie, è possibile sospendere automaticamente l'invio di e-mail che usano i set di configurazione specificati, senza alcun impatto sulle funzionalità globali di invio di e-mail dell'account Amazon SES.

> **Note**
>
> La soluzione descritta in questa sezione permette di sospendere l'invio di e-mail per un set di configurazione specifico in una singola regione AWS. Se invii e-mail da diverse Regioni, ripeti le procedure di questa sezione per ogni Regione in cui desideri implementare questa soluzione.

Argomenti in questa sezione:

Fase 1: abilitazione della segnalazione dei parametri di reputazione per il set di configurazione

Prima di configurare Amazon SES per la sospensione automatica dell'invio di e-mail per un set di configurazione, è necessario abilitare l'esportazione dei parametri di reputazione per il set di configurazione.

Per abilitare l'esportazione dei parametri relativi a mancati recapiti e reclami per il set di configurazione, completa le fasi in the section called “Visualizzazione ed esportazione dei parametri di reputazione”.

Fase 2: creazione di un ruolo IAM

La prima fase per la configurazione della sospensione automatica dell'invio di e-mail consiste nel creare un ruolo IAM in grado di eseguire l'operazione API `UpdateConfigurationSetSendingEnabled`.

Creazione del ruolo IAM

1. Apri la console IAM all'indirizzo https://console.aws.amazon.com/iam/.
2. Nel pannello di navigazione, seleziona Roles (Ruoli).
3. Selezionare Create role (Crea ruolo).
4. In Select type of trusted entity (Seleziona tipo di entità attendibile), scegli AWS service (Servizio AWS).
5. In Choose the service that will use this role (Scegli il servizio che utilizzerà questo ruolo), seleziona Lambda. Seleziona Next: Permissions (Successivo: Autorizzazioni).
6. Nella pagina Attach permissions policies (Collega policy delle autorizzazioni) scegli le policy seguenti:

   - AWS LambdaBasicExecutionRole
   - AmazonSESFullAccess

   > **Tip**
   >
   > Usa la casella di ricerca nella parte superiore dell'elenco delle policy per individuarle rapidamente.

   Seleziona Next: Review (Successivo: Rivedi).
7. Nella pagina Review (Rivedi) per Name (Nome) digita un nome per il ruolo. Scegliere Crea ruolo.

Fase 3: creazione della funzione Lambda

Dopo aver creato un ruolo IAM, è possibile creare la funzione Lambda per la sospensione dell'invio di e-mail per il set di configurazione.

Creazione della funzione Lambda

1. Apri la console AWS Lambda all'indirizzo https://console.aws.amazon.com/lambda/.
2. Usa il selettore della Regione per scegliere la Regione in cui desideri distribuire questa funzione Lambda.

   > **Note**
   >
   > Questa funzione sospende l'invio di e-mail solo per i set di configurazione nella regione AWS selezionata in questa fase. Se invii e-mail da più Regioni, ripeti le procedure di questa sezione per ogni Regione in cui desideri che venga sospeso automaticamente l'invio di e-mail.

3. Seleziona Create function (Crea funzione).
4. In Create function (Crea funzione), scegli Author from scratch (Crea da zero).
5. In Author from scratch (Crea da zero) completa le fasi seguenti:

   - Per Name (Nome) digita un nome per la funzione Lambda.
   - Per Runtime (Tempo di esecuzione), scegli Node.js 14 (o la versione attualmente disponibile nell'elenco selezionato).
   - Per Role (Ruolo) scegli Choose an existing role (Scegli un ruolo esistente).
   - Per Existing role (Ruolo esistente) scegli il ruolo IAM creato in the section called “Fase 2: creazione di un ruolo IAM”.

   Scegli Create function (Crea funzione).
6. In Function code (Codice funzione), nell'editor di codice, incolla il codice seguente:

```
'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);
        }
    });
};
```

Sostituisci *ConfigSet* nel codice precedente con il nome del set di configurazione. Scegli Save (Salva).

7. Scegli Test (Esegui test). Se viene visualizzata la finestra Configure test event (Configura evento test), digita un nome nel campo Event name (Nome evento), quindi scegli Create (Crea).
8. Verifica che nella barra di notifica nella parte superiore della pagina sia visualizzato il messaggio `Execution result: succeeded`. Se l'esecuzione della funzione non è riuscita, procedi nel seguente modo:

   - Verifica che il ruolo IAM creato in the section called “Fase 2: creazione di un ruolo IAM” contenga le policy corrette.
   - Verifica che il codice nella funzione Lambda non contenga errori. L'editor di codice Lambda evidenzia automaticamente gli errori di sintassi e altri potenziali problemi.

Fase 4: riabilitazione dell'invio di e-mail per il set di configurazione

Un effetto secondario dei test della funzione Lambda in the section called “Fase 3: creazione della funzione Lambda” è la sospensione dell'invio di e-mail per il set di configurazione. Nella maggior parte dei casi, è preferibile non sospendere l'invio per il set di configurazione finché non viene attivato l'allarme CloudWatch.

Le procedure in questa sezione permettono di riabilitare l'invio di e-mail per il set di configurazione. Per completare questa procedura, è necessario installare e configurare AWS Command Line Interface. Per ulteriori informazioni, consultare la Guida per l'utente di AWS Command Line Interface.

Riabilitazione dell'invio di e-mail

1. Nella riga di comando, digita il comando seguente per riabilitare l'invio di e-mail per il set di configurazione:

   ```
   aws ses update-configuration-set-sending-enabled \
   --configuration-set-name ConfigSet \
   --enabled
   ```

   Nel comando precedente, sostituisci *ConfigSet* con il nome del set di configurazione per cui desideri sospendere l'invio di e-mail.

2. Nella riga di comando, digita il comando seguente per controllare che l'invio di e-mail sia abilitato:

   ```
   aws ses describe-configuration-set \
   --configuration-set-name ConfigSet \
   --configuration-set-attribute-names reputationOptions
   ```

   Il comando produce output analogo all'esempio seguente:

   ```
   {
       "ConfigurationSet": {
           "Name": "ConfigSet"
       },
       "ReputationOptions": {
           "ReputationMetricsEnabled": true,
           "SendingEnabled": true
       }
   }
   ```

   Se il valore di `SendingEnabled` è `true`, l'invio di e-mail per il set di configurazione è stato riabilitato correttamente.

Fase 5: creazione di un argomento Amazon SNS

Affinché CloudWatch esegua la funzione Lambda quando viene attivato un allarme, è prima necessario creare un argomento Amazon SNS e sottoscrivere la funzione Lambda per l'argomento.

Creazione dell'argomento Amazon SNS

1. Apri la console Amazon SNS all'indirizzo https://console.aws.amazon.com/sns/v3/home.
2. Usa il selettore della Regione per scegliere la Regione in cui desideri che l'invio di e-mail venga sospeso automaticamente.
3. Nel pannello di navigazione, scegli Topics (Argomenti).
4. Scegli Create new topic (Crea nuovo argomento).
5. Nella finestra Create new topic (Crea nuovo argomento), per Topic name (Nome argomento), digita un nome per l'argomento. Facoltativamente, puoi digitare un nome più descrittivo nel campo Display name (Nome visualizzato).

   Scegli Create topic (Crea argomento).
6. Nell'elenco degli argomenti seleziona la casella accanto all'argomento creato nella fase precedente. Dal menu Actions (Operazioni), scegli Subscribe to topic (Sottoscrivi all'argomento).
7. Nella finestra Create subscription (Crea sottoscrizione), esegui le scelte seguenti:
   - In Protocol (Protocollo), seleziona AWS Lambda.
   - Per Endpoint scegli la funzione Lambda creata in the section called “Fase 3: creazione della funzione Lambda”.
   - Per Version or alias (Versione o alias) scegli default (predefinito).
8. Scegli Create Subscription (Crea sottoscrizione).

Fase 6: creazione di un allarme CloudWatch

In questa sezione sono incluse le procedure per la creazione di un allarme in CloudWatch che viene attivato quando un parametro raggiunge una determinata soglia. Quando l'allarme viene attivato, recapita una notifica all'argomento Amazon SNS creato in the section called “Fase 5: creazione di un argomento Amazon SNS”, che quindi esegue la funzione Lambda creata in the section called “Fase 3: creazione della funzione Lambda”.

Creazione di un allarme CloudWatch

1. Apri la console CloudWatch all'indirizzo https://console.aws.amazon.com/cloudwatch/.
2. Usa il selettore della Regione per scegliere la Regione in cui desideri che l'invio di e-mail venga sospeso automaticamente.
3. Nel pannello di navigazione sinistro, scegli Alarms (Allarmi).
4. Scegli Create Alarm (Crea allarme).
5. Nella finestra Create Alarm (Crea allarme), in SES Metrics (Parametri SES), scegli Configuration Set Metrics (Parametri set di configurazione).
6. Nella colonna ses:configuration-set, individua il set di configurazione per cui desideri creare un allarme. In Metric Name (Nome parametro) scegli una delle opzioni seguenti:

   - Reputation.BounceRate: scegli questo parametro se desideri sospendere l'invio di e-mail per il set di configurazione quando la percentuale globale di mancato recapito permanente per il set di configurazione supera una soglia definita.
   - Reputation.ComplaintRate: scegli questo parametro se desideri sospendere l'invio di e-mail per il set di configurazione quando la percentuale globale di reclami per il set di configurazione supera una soglia definita.

   Seleziona Successivo.
7. Completa questa procedura:

   - In Alarm Threshold (Soglia allarme) digita un nome per l'allarme in Name (Nome).
   - In Whenever: Reputation.BounceRate (Ogni volta che: Reputation.BounceRate) o Whenever: Reputation.ComplaintRate (Ogni volta che: Reputation.ComplaintRate), specifica la soglia che causa l'attivazione dell'allarme.

   > **Note**
   >
   > Se la percentuale globale di mancati recapiti per l'account Amazon SES supera il 10%, oppure se la percentuale globale di reclami per l'account Amazon SES supera lo 0,5%, l'account Amazon SES viene automaticamente messo in fase di verifica. Quando specifichi una percentuale di mancati recapiti o reclami che comporta l'attivazione dell'allarme CloudWatch, ti consigliamo di usare valori decisamente inferiori a queste percentuali, per evitare che l'account venga messo in fase di verifica.

- In Actions (Operazioni), in Whenever this alarm (Ogni volta che questo allarme), scegli State is ALARM (Lo stato è ALLARME). Per Send notification to (Invia notifica a) scegli l'argomento Amazon SNS creato in the section called “Fase 5: creazione di un argomento Amazon SNS”.

Scegli Create Alarm (Crea allarme).

Fase 7: verifica della soluzione

A questo punto, puoi testare l'allarme per verificare che esegua la funzione Lambda quando passa nello stato `ALARM`. Puoi usare il comando `SetAlarmState` nell'API CloudWatch per modificare temporaneamente lo stato dell'allarme.

Le procedure di questa sezione sono facoltative, ma ti consigliamo di completarle per verificare che l'intera soluzione sia configurata correttamente.

Verifica della soluzione

1. Nella riga di comando, digita il comando seguente per controllare lo stato dell'invio di e-mail per il set di configurazione:

```
aws ses describe-configuration-set --configuration-set-name ConfigSet
```

Se l'invio è abilitato per il set di configurazione, verrà visualizzato l'output seguente:

```
{
    "ConfigurationSet": {
        "Name": "ConfigSet"
    },
    "ReputationOptions": {
        "ReputationMetricsEnabled": true,
        "SendingEnabled": true
    }
}
```

Se il valore di `SendingEnabled` è `true`, l'invio di e-mail per il set di configurazione è attualmente abilitato.

2. Nella riga di comando, digita il comando seguente per modificare temporaneamente lo stato di allarme in `ALARM`:

```
aws cloudwatch set-alarm-state \
--alarm-name MyAlarm \
--state-value ALARM \
--state-reason "Testing execution of Lambda function"
```

Sostituisci *MyAlarm* nel comando precedente con il nome per l'allarme creato in the section called “Fase 6: creazione di un allarme CloudWatch”.

> **Note**
>
> Quando esegui questo comando, lo stato dell'allarme passa da OK a ALARM e torna a OK entro pochi secondi. Puoi vedere queste modifiche dello stato nella scheda History (Cronologia) dell'allarme nella console CloudWatch oppure con l'operazione DescribeAlarmHistory.

3. Nella riga di comando, digita il comando seguente per controllare lo stato dell'invio di e-mail per il set di configurazione:

```
aws ses describe-configuration-set \
--configuration-set-name ConfigSet
```

Se la funzione Lambda viene eseguita correttamente, viene visualizzato un output analogo al seguente esempio:

```
{
    "ConfigurationSet": {
        "Name": "ConfigSet"
    },
    "ReputationOptions": {
        "ReputationMetricsEnabled": true,
        "SendingEnabled": false
    }
}
```

Se il valore di `SendingEnabled` è `false`, l'invio di e-mail per il set di configurazione è disabilitato e ciò indica che la funzione Lambda è stata eseguita correttamente.

4. Completa le fasi in the section called “Fase 4: riabilitazione dell'invio di e-mail per il set di configurazione” per riabilitare l'invio di e-mail per il set di configurazione.

Monitoraggio degli eventi SES tramite Amazon EventBridge

EventBridge è un servizio serverless che utilizza gli eventi per connettere tra loro i componenti delle applicazioni, semplificando la creazione di applicazioni scalabili basate sugli eventi. L'architettura basata sugli eventi è uno stile di creazione di sistemi software ad accoppiamento debole che interagiscono emettendo e rispondendo agli eventi. Gli eventi sono messaggi in formato JSON che rappresentano tipicamente una modifica in una risorsa o ambiente, o altri eventi di gestione.

Alcune funzionalità di SES generano e inviano eventi al bus eventi predefinito. EventBridge Un router di eventi è un router che riceve eventi e li invia a nessuna o a più destinazioni o target. Le regole associate al router di eventi valutano gli eventi man mano che arrivano. Ogni regola verifica se un evento corrisponde allo schema della regola. Se l'evento corrisponde, EventBridge invia l'evento ai target specificati.

SES invia eventi a EventBridge quando una funzionalità subisce un cambio di stato o un aggiornamento dello stato. È possibile utilizzare EventBridge le regole per indirizzare gli eventi verso obiettivi definiti. Questi eventi verranno recapitati sulla base del miglior tentativo e potrebbero essere recapitati non in ordine.

Argomenti

Eventi SES

I seguenti eventi vengono generati dalle funzionalità SES e inviati al bus di eventi predefinito in EventBridge. Per ulteriori informazioni, compresi i dati di dettaglio per ogni tipo di evento, vedere???.

Eventi per consulenti di Virtual Deliverability Manager

Tipo di evento	Descrizione
Stato del suggerimento dell'advisor Aperto	Un evento viene generato ogni volta che viene aperto un nuovo suggerimento nell'advisor Gestore virtuale della deliverability delle email.

Tipo di evento	Descrizione
Stato del suggerimento dell'advisor Risolto	Un evento viene generato ogni volta che viene risolto un suggerimento nell'advisor Gestore virtuale della deliverability delle email.

Eventi di invio di e-mail SES

Tipo di evento	Descrizione
Email respinta	Un hard bounce che indica che il server di posta del destinata rio ha rifiutato definitivamente l'e-mail. (Le e-mail non recapitate sono incluse solo quando SES non riesce a inviare l’e-mail dopo tentativi ripetuti per un determinato periodo di tempo).
E-mail cliccata	Il destinatario ha fatto clic su uno o più link nell'e-mail.
Reclamo via e-mail ricevuto	L'e-mail è stata recapitata correttamente al server di posta del destinatario, ma il destinatario l'ha contrassegnata come spam.
Consegna di e-mail	SES ha inviato correttamente l'e-mail al server di posta del destinatario.
Consegna e-mail ritardata	Non è stato possibile recapitare l'e-mail al server di posta del destinatario a causa di un problema temporaneo. I ritardi di consegna possono verificarsi, ad esempio quando la casella di posta in arrivo del destinatario è piena o quando nel server di ricezione della posta elettronica si verifica un problema transitor io.
Email aperta	Il destinatario ha ricevuto il messaggio e lo ha aperto nel proprio client di posta elettronica.
Email rifiutata	SES ha accettato l'e-mail, ma ha stabilito che conteneva un virus e non ha cercato di recapitarla al server di posta del destinatario.
Rendering delle e-mail non riuscito	L'e-mail non è stata inviata a causa di un problema di rendering del modello. Questo tipo di evento può verificarsi se i dati del modello mancano o se non vi è corrispondenza tra i parametri e

Tipo di evento	Descrizione
	i dati del modello. Questo tipo di evento si verifica solo quando invii un'e-mail basata su modello utilizzando le operazioni API `SendTemplatedEmail` o `SendBulkTemplatedEmail`.
Email inviata	La richiesta di invio ha avuto esito positivo e SES tenterà di recapitare il messaggio al server di posta del destinatario. Se viene utilizzata l'eliminazione globale o a livello di account, SES la conteggia comunque come invio, ma la consegna viene eliminata.
Email sottoscritta	L'e-mail è stata recapitata correttamente, ma il destinatario ha aggiornato le preferenze di abbonamento facendo clic sull'`List-Unsubscribe` intestazione dell'e-mail o sul `Unsubscribe` collegamento a piè di pagina.

Riferimento allo schema degli eventi SES

Tutti gli eventi generati dai AWS servizi dispongono di un set comune di campi contenenti metadati relativi all'evento, ad esempio il AWS servizio che è all'origine dell'evento, l'ora in cui l'evento è stato generato, l'account e la regione in cui si è svolto l'evento e altri. Per le definizioni di questi campi generali, consultate il riferimento alla struttura degli eventi nella Guida per l'EventBridge utente.

Inoltre, ogni evento ha un campo `detail` che contiene dati specifici per quel particolare evento. Il riferimento seguente definisce i campi di dettaglio per i vari eventi SES.

Quando si utilizza EventBridge per selezionare e gestire gli eventi SES, è utile tenere presente quanto segue:

- Il campo `source` per tutti gli eventi SES è impostato su `aws.ses`.
- Il campo `detail-type` specifica il tipo di evento. Consulta la tabella dei tipi di evento inthe section called “Eventi SES”.
- Il campo `detail` contiene i dati specifici di quel particolare evento.

  Per alcuni tipi di eventi, come quelli per Virtual Deliverability Manager, il campo di dettaglio è una stringa di dati piuttosto semplicistica che viene popolata da un insieme finito di valori statici. Al contrario, il campo di dettaglio per gli eventi di invio di e-mail è più complesso in quanto può essere

costituito da molti sottocampi di dettaglio che sono una combinazione di valori statici e dinamici come il timestamp di quando è stata inviata un'e-mail, l'indirizzo del destinatario e molti altri attributi di posta elettronica.

Argomenti

Schema dello stato dell'advisor Gestore virtuale della deliverability delle email

Il seguente riferimento allo schema definisce i campi specifici degli eventi di stato del consulente di Virtual Deliverability Manager.

Le definizioni per i campi generali che compaiono in tutti gli schemi di eventi (come *`version`*, *`idaccount`*, e altri) sono disponibili nel riferimento alla struttura degli eventi nella Guida per l'EventBridge utente. I campi `source` e `detail-type` sono inclusi nel riferimento seguente perché contengono valori specifici di SES per gli eventi SES.

`source`

Identifica il servizio che ha generato l'evento. Per gli eventi SES, questo valore è `aws.ses`.

`detail-type`

Identifica il tipo di evento.

I valori di questo campo sono elencati nella tabella degli eventi del consulente di Virtual Deliverability Manager in. the section called “Eventi SES”

`detail`

Un oggetto JSON contenente informazioni sull'evento. Il servizio che genera l'evento determina il contenuto di questo campo.

I valori per questo campo possono essere:

- `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 Esempio: evento di stato dell'advisor Gestore virtuale della deliverability delle email

Di seguito è riportato un esempio di evento di stato dell'advisor Gestore virtuale della deliverability delle email per il tipo di evento `Advisor Recommendation Status Open`. Il valore dell'evento di dettaglio in questo esempio è`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." }
}
```

Schema di stato dell'invio di e-mail SES

Il seguente riferimento allo schema definisce i campi specifici degli eventi di stato dell'invio di e-mail SES.

Le definizioni per i campi generali che compaiono in tutti gli schemi di eventi (come`version`, `idaccount`, e altri) sono disponibili nel riferimento alla struttura degli eventi nella Guida per l'EventBridge utente. I campi `source` e `detail-type` sono inclusi nel riferimento seguente perché contengono valori specifici di SES per gli eventi SES.

`source`

Identifica il servizio che ha generato l'evento. Per gli eventi SES, questo valore è `aws.ses`.

`detail-type`

Identifica il tipo di evento.

I valori di questo campo sono elencati nella tabella degli eventi di invio e-mail di SES inthe section called “Eventi SES”.

`detail`

Un oggetto JSON contenente informazioni sull'evento. Il servizio che genera l'evento determina il contenuto di questo campo.

Tutti i valori possibili per questo campo non possono essere elencati qui perché comprendono valori statici e dinamici generati da ogni e-mail univoca inviata in un dato momento. Tuttavia, viene fornito un esempio per darti un'idea del tipo di dati che questo campo può contenere. È possibile trovare dati di dettaglio di esempio per tutti i tipi di eventi di invio di e-mail utilizzando la EventBridge Sandbox, vediSpecificate un evento di esempio in EventBridge.

Un esempio di dati di dettaglio generati per l'evento `Email Rendering Failed` di invio e-mail 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 Esempio: evento sullo stato dell'invio di e-mail

Di seguito è riportato un esempio dell'evento completo sullo stato dell'invio di e-mail per il tipo di eventoEmail Rendering Failed. Il valore dell'evento di dettaglio in questo esempio è una combinazione di valori statici e dinamici basati sull'evento di invio e-mail per un'e-mail specifica.

```
{
  "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"
```

```
    }
  }
}
```

Utilizzo EventBridge con eventi SES

Per impostazione predefinita, SES invia gli eventi al bus eventi EventBridge predefinito. È possibile creare regole sul bus degli eventi predefinito per identificare eventi specifici EventBridge da inviare a uno o più obiettivi specifici. Ogni regola contiene uno schema di eventi che EventBridge viene utilizzato per abbinare gli eventi man mano che arrivano sul bus degli eventi. Se un evento corrisponde allo schema di eventi per una determinata regola, EventBridge invia l'evento al target specificato nella regola.

Nel EventBridge, la definizione di un modello di evento fa in genere parte del processo più ampio di creazione di una nuova regola o di modifica di una regola esistente. Per informazioni su come creare EventBridge regole, consulta Creazione di EventBridge regole Amazon che reagiscono agli eventi nella Guida per l'EventBridge utente.

Utilizzando la funzionalità Sandbox in EventBridge, puoi definire rapidamente un modello di evento e utilizzare un evento di esempio per confermare che il modello corrisponda agli eventi desiderati, senza dover prima creare o modificare una regola. Per istruzioni dettagliate sull'uso della Sandbox, consulta Testare un pattern di eventi utilizzando la EventBridge Sandbox nella Guida per l'EventBridge utente.

Specificate un evento di esempio SES nella Sandbox EventBridge

È possibile scegliere eventi SES di esempio al fine di testare i modelli di eventi che si stanno creando.

Per specificare un evento di esempio SES nella EventBridge Sandbox

1. Apri la EventBridge console Amazon all'indirizzo https://console.aws.amazon.com/events/.
2. Nel riquadro di navigazione, scegli Risorse per gli sviluppatori, quindi seleziona Sandbox e nella pagina Sandbox scegli la scheda Modello di eventi.
3. Per Event source, scegli AWS eventi o eventi EventBridge partner.
4. Nella sezione Evento di esempio, per Tipo evento di esempio, seleziona Eventi AWS .
5. Per Eventi di esempio, scorri verso il basso fino a SES e seleziona l'evento SES desiderato.

EventBridge visualizza un evento di esempio, insieme a tutti i relativi dati di dettaglio, per il tipo di evento.

È quindi possibile utilizzare questo evento per testare il modello di evento creato nella sezione Schema di eventi o utilizzarlo come base per creare eventi di esempio personalizzati per il test dei pattern descritti nella sezione seguente.

Creazione e test di modelli di eventi SES

Dopo aver selezionato un evento di esempio, come spiegato nella sezione precedente, potete creare un modello di evento e utilizzare l'evento di esempio per assicurarvi che corrisponda agli eventi desiderati.

Per creare e testare un pattern di eventi che corrisponda agli eventi SES nella EventBridge Sandbox

1. Apri la EventBridge console Amazon all'indirizzo https://console.aws.amazon.com/events/.
2. Nel riquadro di navigazione, scegli Risorse per gli sviluppatori, quindi seleziona Sandbox e nella pagina Sandbox scegli la scheda Modello di eventi.
3. Per Event source, scegli AWS eventi o eventi EventBridge partner e seleziona l'evento di esempio che desideri testare come spiegato nella sezione precedente.
4. Scorri verso il basso fino a Metodo di creazione e scegli Usa modulo modello.
5. Nella sezione Modello di eventi, per Origine evento scegli Servizi AWS .
6. In AWS servizio, seleziona SES.
7. Per Tipo di evento seleziona il tipo di evento SES di cui desideri eseguire la corrispondenza.

   EventBridge visualizza lo schema di eventi minimo, composto da `source` e `detail-type` campi, che corrisponde all'evento SES selezionato.

   Nei due esempi, il primo schema di eventi corrisponde a tutti `Advisor Recommendation Status Resolved` gli eventi e nel secondo a tutti gli `Email Bounced` eventi:

   ```
   {
     "source": ["aws.ses"],
     "detail-type": ["Advisor Recommendation Status Resolved"]
   }
   ```

```
{
  "source": ["aws.ses"],
  "detail-type": ["Email Bounced"]
}
```

8. Per apportare modifiche al pattern di eventi, seleziona Modifica pattern e apporta le modifiche nell'editor JSON.

   È anche possibile effettuare corrispondenze con i valori presenti in uno o più campi dei dati dettagliati. Ciò include la specifica di valori multipli possibili per un valore di campo.

   Nell'esempio seguente, il campo di dettaglio è stato aggiunto al modello di evento minimo generato con il valore del `data` campo specificato per trovare tutti gli eventi del consulente di Virtual Deliverability Manager con lo stesso valore di dettaglio: `DKIM record was not found`

```
{
  "source": ["aws.ses"],
  "detail-type": ["Advisor Recommendation Status Resolved"],
  "detail": {
    "data": ["DKIM record was not found."]
  }
}
```

   In questo esempio, i sottocampi di dettaglio sono stati aggiunti al rapporto sugli eventi generati da tutte le e-mail inviate da noreply@example.com il 5 agosto 2024 che sono state respinte. (La corrispondenza dei prefissi viene utilizzata qui come parte del filtraggio dei contenuti.):

```
{
  "source": ["aws.ses"],
  "detail-type": ["Email Bounced"],
  "detail": {
    "mail": {
      "timestamp": [{
        "prefix": "2024-08-05"
      }],
      "source": ["noreply@example.com"]
    }
  }
}
```

È importante leggere i pattern di eventi nella Guida per l'EventBridge utente: spiega che il valore del modello di evento che inserisci nell'editor JSON deve essere racchiuso tra parentesi quadre `[...]` perché è considerato un array. Vengono inoltre fornite queste e altre informazioni su come costruire modelli di eventi avanzati.

9. Per verificare se il modello di evento corrisponde all'evento di esempio specificato nel riquadro di eventi di esempio precedente, seleziona Test pattern. Se corrisponde, verrà visualizzato un banner verde nella parte inferiore dell'editor JSON, «L'evento di esempio corrisponde al modello di evento».
10. Per risolvere gli errori dopo aver selezionato Test pattern:
    - Se sono presenti errori relativi a JSON, il messaggio indicherà il motivo, ad esempio «Il modello di evento non è valido. Motivo: «dati» deve essere un oggetto o una matrice alla riga: 5, colonna: 14". Per ovviare a ciò, racchiudi il valore sulla riga 5 tra parentesi quadre. `[...]`
    - Se c'è una discrepanza tra i valori dell'evento Sample e il pattern dell'evento, il messaggio sarà «L'evento di esempio non corrisponde al pattern dell'evento». Ciò significa che uno o più valori che vuoi testare sono diversi dai valori di esempio generati dal generatore di eventi Sample. Per ovviare a questo problema, procedi con i passaggi rimanenti.
11. Per modificare i valori di esempio nell'evento Sample in modo da testare correttamente il modello di evento, nel riquadro Sample event, seleziona Copia nell'editor JSON.
12. Seleziona il pulsante di opzione accanto al tipo di evento Enter my own for Sample sopra l'editor.
13. Incolla l'evento di esempio nell'editor JSON e, per qualsiasi campo che utilizzi nel modello di evento, sostituisci il valore dello stesso campo in modo che corrisponda al valore specificato nel modello di evento.
14. Scorri verso il basso fino al riquadro Event pattern e seleziona nuovamente Test pattern. Se tutti i valori sono stati inseriti correttamente e corrispondono, verrà visualizzato un banner verde nella parte inferiore dell'editor JSON, «L'evento di esempio corrisponde al modello di evento».

Risorse aggiuntive EventBridge

Consulta i seguenti argomenti nella Amazon EventBridge User Guide per ulteriori informazioni su come utilizzare EventBridge per elaborare e gestire gli eventi.

- Per informazioni dettagliate su come funzionano i bus di eventi, consulta Amazon EventBridge Event Bus.

- Per informazioni sulla struttura degli eventi, consulta la sezione Eventi
- Per informazioni sulla creazione di modelli di eventi EventBridge da utilizzare per abbinare gli eventi alle regole, consulta Event pattern
- Per informazioni sulla creazione di regole per specificare quali eventi vengono EventBridge elaborati, consulta Regole
- Per informazioni su come specificare a quali servizi o altre destinazioni EventBridge inviano gli eventi corrispondenti, consulta Target

Esempi di codice per Amazon SES con SDK AWS

I seguenti esempi di codice mostrano come utilizzare Amazon SES con un Software Development Kit (SDK) AWS.

Per un elenco completo delle guide per gli sviluppatori di SDK AWS ed esempi di codice, consulta la sezione Utilizzo di Amazon SES con un AWS SDK. Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Esempi di codice

    - Utilizzo SendEmail con un AWS SDK o una CLI
- Scenari per Amazon SES API v2 con SDK AWS
    - Un flusso di lavoro completo per la newsletter di Amazon SES API v2 utilizzando un SDK AWS

Esempi di codice per Amazon SES con AWS SDK

I seguenti esempi di codice mostrano come usare Amazon SES con un kit di sviluppo AWS software (SDK).

Le operazioni sono estratti di codice da programmi più grandi e devono essere eseguite nel contesto. Sebbene le operazioni mostrino come richiamare le singole funzioni del servizio, è possibile visualizzarle contestualizzate negli scenari correlati e negli esempi tra servizi.

Scenari: esempi di codice che mostrano come eseguire un'attività specifica richiamando più funzioni all'interno dello stesso servizio.

Esempi cross-service: applicazioni di esempio che funzionano su più servizi Servizi AWS.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. Utilizzo di Amazon SES con un AWS SDK Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Esempi di codice

- Azioni per Amazon SES tramite AWS SDK
    - Utilizzo CreateReceiptFilter con un AWS SDK o una CLI
    - Utilizzo CreateReceiptRule con un AWS SDK o una CLI
    - Utilizzo CreateReceiptRuleSet con un AWS SDK o una CLI
    - Utilizzo CreateTemplate con un AWS SDK o una CLI
    - Utilizzo DeleteIdentity con un AWS SDK o una CLI
    - Utilizzo DeleteReceiptFilter con un AWS SDK o una CLI
    - Utilizzo DeleteReceiptRule con un AWS SDK o una CLI
    - Utilizzo DeleteReceiptRuleSet con un AWS SDK o una CLI
    - Utilizzo DeleteTemplate con un AWS SDK o una CLI
    - Utilizzo DescribeReceiptRuleSet con un AWS SDK o una CLI

- Utilizzo GetIdentityVerificationAttributes con un AWS SDK o una CLI
- Utilizzo GetSendQuota con un AWS SDK o una CLI
- Utilizzo GetSendStatistics con un AWS SDK o una CLI
- Utilizzo GetTemplate con un AWS SDK o una CLI
- Utilizzo ListIdentities con un AWS SDK o una CLI
- Utilizzo ListReceiptFilters con un AWS SDK o una CLI
- Utilizzo ListTemplates con un AWS SDK o una CLI
- Utilizzo SendBulkTemplatedEmail con un AWS SDK o una CLI
- Utilizzo SendEmail con un AWS SDK o una CLI
- Utilizzo SendRawEmail con un AWS SDK o una CLI
- Utilizzo SendTemplatedEmail con un AWS SDK o una CLI
- Utilizzo UpdateTemplate con un AWS SDK o una CLI
- Utilizzo VerifyDomainIdentity con un AWS SDK o una CLI
- Utilizzo VerifyEmailIdentity con un AWS SDK o una CLI

- Scenari per Amazon SES che utilizzano AWS SDK
  - Copia le identità di e-mail e dominio di Amazon SES da una AWS regione all'altra utilizzando un SDK AWS
  - Generazione di credenziali per eseguire la connessione a un endpoint SMTP di Amazon SES
  - Verifica un'identità e-mail e invia messaggi con Amazon SES utilizzando un AWS SDK
- Esempi di servizi multipli per Amazon SES che utilizzano SDK AWS
  - Creazione di un'app in streaming Amazon Transcribe
  - Creazione di un'applicazione Web per tracciare i dati DynamoDB
  - Come creare un tracker di articoli Amazon Redshift
  - Creazione di un tracciatore di elementi di lavoro di Aurora Serverless
  - Rileva i DPI nelle immagini con Amazon Rekognition utilizzando un SDK AWS
  - Rileva oggetti nelle immagini con Amazon Rekognition utilizzando un SDK AWS
  - Rileva persone e oggetti in un video con Amazon Rekognition utilizzando un SDK AWS
  - Utilizzo di Step Functions per richiamare le funzioni Lambda

Azioni per Amazon SES tramite AWS SDK

I seguenti esempi di codice mostrano come eseguire singole azioni Amazon SES con gli AWS SDK. Questi estratti chiamano l'API Amazon SES e sono estratti di codice da programmi più grandi che devono essere eseguiti in modo contestuale. Ogni esempio include un collegamento a GitHub, dove puoi trovare le istruzioni per la configurazione e l'esecuzione del codice.

Gli esempi seguenti includono solo le operazioni più comunemente utilizzate. Per un elenco completo, consulta la Documentazione di riferimento delle API Amazon Simple Email Service (Amazon SES).

Esempi

- Utilizzo CreateReceiptFilter con un AWS SDK o una CLI
- Utilizzo CreateReceiptRule con un AWS SDK o una CLI
- Utilizzo CreateReceiptRuleSet con un AWS SDK o una CLI
- Utilizzo CreateTemplate con un AWS SDK o una CLI
- Utilizzo DeleteIdentity con un AWS SDK o una CLI
- Utilizzo DeleteReceiptFilter con un AWS SDK o una CLI
- Utilizzo DeleteReceiptRule con un AWS SDK o una CLI
- Utilizzo DeleteReceiptRuleSet con un AWS SDK o una CLI
- Utilizzo DeleteTemplate con un AWS SDK o una CLI
- Utilizzo DescribeReceiptRuleSet con un AWS SDK o una CLI
- Utilizzo GetIdentityVerificationAttributes con un AWS SDK o una CLI
- Utilizzo GetSendQuota con un AWS SDK o una CLI
- Utilizzo GetSendStatistics con un AWS SDK o una CLI
- Utilizzo GetTemplate con un AWS SDK o una CLI
- Utilizzo ListIdentities con un AWS SDK o una CLI
- Utilizzo ListReceiptFilters con un AWS SDK o una CLI
- Utilizzo ListTemplates con un AWS SDK o una CLI
- Utilizzo SendBulkTemplatedEmail con un AWS SDK o una CLI
- Utilizzo SendEmail con un AWS SDK o una CLI
- Utilizzo SendRawEmail con un AWS SDK o una CLI

- Utilizzo SendTemplatedEmail con un AWS SDK o una CLI
- Utilizzo UpdateTemplate con un AWS SDK o una CLI
- Utilizzo VerifyDomainIdentity con un AWS SDK o una CLI
- Utilizzo VerifyEmailIdentity con un AWS SDK o una CLI

Utilizzo **`CreateReceiptFilter`** con un AWS SDK o una CLI

I seguenti esempi di codice mostrano come utilizzare`CreateReceiptFilter`.

C++

SDK per C++

> **Note**
>
> C'è altro su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice 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();
}
```

- Per i dettagli sull'API, CreateReceiptFilterconsulta AWS SDK for C++ API Reference.

JavaScript

SDK per JavaScript (v3)

> **Note**
>
> C'è altro da fare. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice 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;
  }
};
```

- Per i dettagli sull'API, CreateReceiptFilterconsulta AWS SDK for JavaScript API Reference.

Python

SDK per Python (Boto3)

> **Note**
>
> C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice 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
```

- Per i dettagli sull'API, consulta CreateReceiptFilter AWSSDK for Python (Boto3) API Reference.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. Utilizzo di Amazon SES con un AWS SDK Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Utilizzo **`CreateReceiptRule`** con un AWS SDK o una CLI

I seguenti esempi di codice mostrano come utilizzare`CreateReceiptRule`.

C++

SDK per C++

> **Note**
>
> C'è altro su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice 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();
}
```

- Per i dettagli sull'API, CreateReceiptRuleconsulta AWS SDK for C++ API Reference.

JavaScript

SDK per JavaScript (v3)

> **Note**
>
> C'è altro da fare. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice 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;
  }
};
```

- Per i dettagli sull'API, CreateReceiptRuleconsulta AWS SDK for JavaScript API Reference.

Python

SDK per Python (Boto3)

> **Note**
>
> C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

Crea un bucket Simple Storage Service (Amazon S3) in cui Amazon SES può inserire copie delle e-mail in arrivo e crea una regola che copia le e-mail in arrivo nel bucket per un elenco specifico di destinatari.

```
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
```

- Per i dettagli sull'API, consulta CreateReceiptRule AWSSDK for Python (Boto3) API Reference.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. Utilizzo di Amazon SES con un AWS SDK Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Utilizzo **`CreateReceiptRuleSet`** con un AWS SDK o una CLI

I seguenti esempi di codice mostrano come utilizzare`CreateReceiptRuleSet`.

C++

SDK per C++

> **Note**
>
> C'è altro su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice 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();
}
```

- Per i dettagli sull'API, CreateReceiptRuleSetconsulta AWS SDK for C++ API Reference.

JavaScript

SDK per JavaScript (v3)

> **Note**
>
> C'è altro da fare. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice 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;
  }
};
```

- Per i dettagli sull'API, CreateReceiptRuleSetconsulta AWS SDK for JavaScript API Reference.

Python

SDK per Python (Boto3)

> **Note**
>
> C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice 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
```

- Per i dettagli sull'API, consulta CreateReceiptRuleSet AWSSDK for Python (Boto3) API Reference.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. Utilizzo di Amazon SES con un AWS SDK Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Utilizzo **`CreateTemplate`** con un AWS SDK o una CLI

I seguenti esempi di codice mostrano come utilizzare`CreateTemplate`.

Gli esempi di operazioni sono estratti di codice da programmi più grandi e devono essere eseguiti nel contesto. È possibile visualizzare questa operazione nel contesto nel seguente esempio di codice:

- Verifica di un'identità e-mail e invio di messaggi

.NET

AWS SDK for .NET

> **Note**
>
> C'è altro su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice 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;
    }
```

- Per i dettagli sull'API, CreateTemplateconsulta AWS SDK for .NET API Reference.

C++

SDK per C++

> **Note**
>
> C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice 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();
}
```

- Per i dettagli sull'API, CreateTemplateconsulta AWS SDK for C++ API Reference.

JavaScript

SDK per JavaScript (v3)

> **Note**
>
> C'è altro da fare. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice 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;
  }
};
```

- Per i dettagli sull'API, CreateTemplateconsulta AWS SDK for JavaScript API Reference.

Python

SDK per Python (Boto3)

> **Note**
>
> C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice 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
```

- Per i dettagli sull'API, consulta CreateTemplate AWSSDK for Python (Boto3) API Reference.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. Utilizzo di Amazon SES con un AWS SDK Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Utilizzo **`DeleteIdentity`** con un AWS SDK o una CLI

I seguenti esempi di codice mostrano come utilizzare`DeleteIdentity`.

Gli esempi di operazioni sono estratti di codice da programmi più grandi e devono essere eseguiti nel contesto. È possibile visualizzare questa operazione nel contesto nel seguente esempio di codice:

- Verifica di un'identità e-mail e invio di messaggi

.NET

AWS SDK for .NET

> **Note**
>
> C'è altro su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice 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;
    }
```

- Per i dettagli sull'API, DeleteIdentityconsulta AWS SDK for .NET API Reference.

C++

SDK per C++

> **Note**
>
> C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice 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();
}
```

- Per i dettagli sull'API, DeleteIdentityconsulta AWS SDK for C++ API Reference.

CLI

AWS CLI

Eliminazione di un'identità

Nell'esempio seguente viene utilizzato il comando `delete-identity` per eliminare un'identità dall'elenco delle identità verificate con Amazon SES:

```
aws ses delete-identity --identity user@example.com
```

Per ulteriori informazioni riguardo alle identità verificate, consulta Verifica degli indirizzi e-mail e dei domini in Amazon SES nella Guida per gli sviluppatori di Amazon Simple Email Service.

- Per i dettagli sull'API, consulta DeleteIdentity AWS CLICommand Reference.

JavaScript

SDK per JavaScript (v3)

> **Note**
>
> C'è altro da fare. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice 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;
  }
};
```

- Per i dettagli sull'API, DeleteIdentityconsulta AWS SDK for JavaScript API Reference.

Python

SDK per Python (Boto3)

> **Note**
>
> C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice 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
```

- Per i dettagli sull'API, consulta DeleteIdentity AWSSDK for Python (Boto3) API Reference.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. Utilizzo di Amazon SES con un AWS SDK Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Utilizzo **`DeleteReceiptFilter`** con un AWS SDK o una CLI

I seguenti esempi di codice mostrano come utilizzare`DeleteReceiptFilter`.

C++

SDK per C++

> **Note**
>
> C'è altro su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice 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();
}
```

- Per i dettagli sull'API, DeleteReceiptFilterconsulta AWS SDK for C++ API Reference.

JavaScript

SDK per JavaScript (v3)

> **Note**
>
> C'è altro da fare. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice 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;
  }
};
```

- Per i dettagli sull'API, DeleteReceiptFilterconsulta AWS SDK for JavaScript API Reference.

Python

SDK per Python (Boto3)

> **Note**
>
> C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice 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
```

- Per i dettagli sull'API, consulta DeleteReceiptFilter AWSSDK for Python (Boto3) API Reference.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. Utilizzo di Amazon SES con un AWS SDK Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Utilizzo **`DeleteReceiptRule`** con un AWS SDK o una CLI

I seguenti esempi di codice mostrano come utilizzare`DeleteReceiptRule`.

C++

SDK per C++

> **Note**
>
> C'è altro su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice 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();
}
```

- Per i dettagli sull'API, DeleteReceiptRuleconsulta AWS SDK for C++ API Reference.

JavaScript

SDK per JavaScript (v3)

> **Note**
>
> C'è altro da fare. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice 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;
  }
};
```

- Per i dettagli sull'API, DeleteReceiptRuleconsulta AWS SDK for JavaScript API Reference.

Python

SDK per Python (Boto3)

> **Note**
>
> C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice 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
```

- Per i dettagli sull'API, consulta DeleteReceiptRule AWSSDK for Python (Boto3) API Reference.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. Utilizzo di Amazon SES con un AWS SDK Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Utilizzo **`DeleteReceiptRuleSet`** con un AWS SDK o una CLI

I seguenti esempi di codice mostrano come utilizzare`DeleteReceiptRuleSet`.

C++

SDK per C++

> **Note**
>
> C'è altro su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice 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();
}
```

- Per i dettagli sull'API, DeleteReceiptRuleSetconsulta AWS SDK for C++ API Reference.

JavaScript

SDK per JavaScript (v3)

> **Note**
>
> C'è altro da fare. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice 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;
  }
};
```

- Per i dettagli sull'API, DeleteReceiptRuleSetconsulta AWS SDK for JavaScript API Reference.

Python

SDK per Python (Boto3)

> **Note**
>
> C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice 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
```

- Per i dettagli sull'API, consulta DeleteReceiptRuleSet AWSSDK for Python (Boto3) API Reference.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. Utilizzo di Amazon SES con un AWS SDK Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Utilizzo **`DeleteTemplate`** con un AWS SDK o una CLI

I seguenti esempi di codice mostrano come utilizzare`DeleteTemplate`.

Gli esempi di operazioni sono estratti di codice da programmi più grandi e devono essere eseguiti nel contesto. È possibile visualizzare questa operazione nel contesto nel seguente esempio di codice:

- Verifica di un'identità e-mail e invio di messaggi

.NET

AWS SDK for .NET

> **Note**
>
> C'è altro su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice 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;
    }
```

- Per i dettagli sull'API, DeleteTemplateconsulta AWS SDK for .NET API Reference.

C++

SDK per C++

> **Note**
>
> C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice 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();
}
```

- Per i dettagli sull'API, DeleteTemplateconsulta AWS SDK for C++ API Reference.

JavaScript

SDK per JavaScript (v3)

> **Note**
>
> C'è altro da fare. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice 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;
```

```
  }
};
```

- Per i dettagli sull'API, DeleteTemplateconsulta AWS SDK for JavaScript API Reference.

Python

SDK per Python (Boto3)

> **Note**
>
> C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice 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
```

- Per i dettagli sull'API, consulta DeleteTemplate AWSSDK for Python (Boto3) API Reference.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. Utilizzo di Amazon SES con un AWS SDK Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Utilizzo **`DescribeReceiptRuleSet`** con un AWS SDK o una CLI

Il seguente esempio di codice mostra come utilizzare`DescribeReceiptRuleSet`.

Python

SDK per Python (Boto3)

> **Note**
>
> C'è altro su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice 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
```

- Per i dettagli sull'API, consulta DescribeReceiptRuleSet AWSSDK for Python (Boto3) API Reference.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. Utilizzo di Amazon SES con un AWS SDK Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Utilizzo **`GetIdentityVerificationAttributes`** con un AWS SDK o una CLI

I seguenti esempi di codice mostrano come utilizzare`GetIdentityVerificationAttributes`.

Gli esempi di operazioni sono estratti di codice da programmi più grandi e devono essere eseguiti nel contesto. È possibile visualizzare questa operazione nel contesto nel seguente esempio di codice:

- Verifica di un'identità e-mail e invio di messaggi

.NET

AWS SDK for .NET

> **Note**
>
> C'è altro su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice 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;
   }
```

- Per i dettagli sull'API, GetIdentityVerificationAttributesconsulta AWS SDK for .NET API Reference.

CLI

AWS CLI

Ottenere lo stato di verifica di Amazon SES per un elenco di identità

Nell'esempio seguente viene utilizzato il comando `get-identity-verification-attributes` per richiamare lo stato di verifica di Amazon SES per un elenco di identità:

```
aws ses get-identity-verification-attributes --identities "user1@example.com"
 "user2@example.com"
```

Output:

```
{
   "VerificationAttributes": {
       "user1@example.com": {
           "VerificationStatus": "Success"
       },
       "user2@example.com": {
           "VerificationStatus": "Pending"
       }
   }
}
```

Se chiami questo comando con un'identità che non hai mai inviato per la verifica, tale identità non verrà visualizzata nell'output.

Per ulteriori informazioni riguardo alle identità verificate, consulta Verifica degli indirizzi e-mail e dei domini in Amazon SES nella Guida per gli sviluppatori di Amazon Simple Email Service.

- Per i dettagli sull'API, consulta GetIdentityVerificationAttributes AWS CLICommand Reference.

Python

SDK per Python (Boto3)

> **Note**
>
> C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice 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
```

- Per i dettagli sull'API, consulta GetIdentityVerificationAttributes AWSSDK for Python (Boto3) API Reference.

Ruby

SDK per Ruby

> **Note**
>
> C'è di più su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice 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
```

- Per i dettagli sull'API, GetIdentityVerificationAttributesconsulta AWS SDK for Ruby API Reference.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consultaUtilizzo di Amazon SES con un AWS SDK. Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Utilizzo **`GetSendQuota`** con un AWS SDK o una CLI

I seguenti esempi di codice mostrano come utilizzare`GetSendQuota`.

.NET

AWS SDK for .NET

> **Note**
>
> C'è altro su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice 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;
    }
```

- Per i dettagli sull'API, GetSendQuotaconsulta AWS SDK for .NET API Reference.

CLI

AWS CLI

Ottenere i limiti di invio di Amazon SES

Nell'esempio seguente viene utilizzato il comando `get-send-quota` per restituire i limiti di invio di Amazon SES:

```
aws ses get-send-quota
```

Output:

```
{
   "Max24HourSend": 200.0,
   "SentLast24Hours": 1.0,
   "MaxSendRate": 1.0
}
```

Max24 HourSend è la tua quota di invio, ovvero il numero massimo di email che puoi inviare in un periodo di 24 ore. La quota di invio riflette un periodo di tempo continuo. Ogni volta che provi a inviare un messaggio e-mail, Amazon SES verifica la quantità di e-mail inviate nelle ultime 24 ore. Se il numero totale di e-mail che hai inviato è inferiore alla quota, la tua richiesta sarà accettata e l'e-mail inviata.

SentLast24Hours è il numero di email che hai inviato nelle 24 ore precedenti.

MaxSendRate è il numero massimo di e-mail che puoi inviare al secondo.

Tieni presente che i limiti di invio si basano sui destinatari e non sui messaggi. Ad esempio, un'e-mail con 10 destinatari viene conteggiata come 10 e-mail ai fini della quota sugli invii.

Per ulteriori informazioni, consulta Gestione dei limiti di invio in Amazon SES nella Guida per gli sviluppatori di Amazon Simple Email Service.

- Per i dettagli sull'API, consulta GetSendQuota AWS CLICommand Reference.

PowerShell

Strumenti per PowerShell

Esempio 1: questo comando restituisce i limiti di invio correnti dell'utente.

```
Get-SESSendQuota
```

- Per i dettagli sull'API, vedere GetSendQuotain AWS Tools for PowerShell Cmdlet Reference.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. Utilizzo di Amazon SES con un AWS SDK Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Utilizzo **`GetSendStatistics`** con un AWS SDK o una CLI

I seguenti esempi di codice mostrano come utilizzare`GetSendStatistics`.

CLI

AWS CLI

Per ottenere le statistiche di invio di Amazon SES

L'esempio seguente utilizza il `get-send-statistics` comando per restituire le statistiche di invio di Amazon SES

```
aws ses get-send-statistics
```

Output:

```
{
   "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
        }
    ]
}
```

Il risultato è un elenco di punti dati, che rappresentano le ultime due settimane di attività di invio. Ogni punto dati nell'elenco contiene statistiche per un intervallo di 15 minuti.

In questo esempio, ci sono solo due punti dati perché le uniche e-mail inviate dall'utente nelle ultime due settimane rientrano in due intervalli di 15 minuti.

Per ulteriori informazioni, consulta Monitoring Your Your Amazon SES Usage Statistics nella Amazon Simple Email Service Developer Guide.

- Per i dettagli sull'API, consulta GetSendStatistics AWS CLICommand Reference.

PowerShell

Strumenti per PowerShell

Esempio 1: questo comando restituisce le statistiche di invio dell'utente. Il risultato è un elenco di punti dati, che rappresentano le ultime due settimane di attività di invio. Ogni punto dati nell'elenco contiene statistiche per un intervallo di 15 minuti.

```
Get-SESSendStatistic
```

- Per i dettagli sull'API, vedere GetSendStatisticsin AWS Tools for PowerShell Cmdlet Reference.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. Utilizzo di Amazon SES con un AWS SDK Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Utilizzo **`GetTemplate`** con un AWS SDK o una CLI

I seguenti esempi di codice mostrano come utilizzare`GetTemplate`.

Gli esempi di operazioni sono estratti di codice da programmi più grandi e devono essere eseguiti nel contesto. Puoi vedere questa azione nel contesto nel seguente esempio di codice:

- Verifica di un'identità e-mail e invio di messaggi

C++

SDK per C++

> **Note**
>
> C'è altro su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice 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();
}
```

- Per i dettagli sull'API, GetTemplateconsulta AWS SDK for C++ API Reference.

JavaScript

SDK per JavaScript (v3)

> **Note**
>
> C'è altro da fare. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice 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;
  }
};
```

- Per i dettagli sull'API, GetTemplateconsulta AWS SDK for JavaScript API Reference.

Python

SDK per Python (Boto3)

> **Note**
>
> C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice 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
```

- Per i dettagli sull'API, consulta GetTemplate AWSSDK for Python (Boto3) API Reference.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. Utilizzo di Amazon SES con un AWS SDK Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Utilizzo **`ListIdentities`** con un AWS SDK o una CLI

I seguenti esempi di codice mostrano come utilizzare`ListIdentities`.

Gli esempi di operazioni sono estratti di codice da programmi più grandi e devono essere eseguiti nel contesto. È possibile visualizzare questa operazione nel contesto nei seguenti esempi di codice:

- Copia delle identità domini ed e-mail tra Regioni
- Verifica di un'identità e-mail e invio di messaggi

.NET

AWS SDK for .NET

> **Note**
>
> C'è altro su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice 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;
   }
```

- Per i dettagli sull'API, ListIdentitiesconsulta AWS SDK for .NET API Reference.

C++

SDK per C++

> **Note**
>
> C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice 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;
}
```

- Per i dettagli sull'API, ListIdentitiesconsulta AWS SDK for C++ API Reference.

CLI

AWS CLI

Per elencare tutte le identità (indirizzi e-mail e domini) di un account specifico AWS

Nell'esempio seguente viene utilizzato il comando `list-identities` per elencare tutte le identità che sono state inviate per la verifica con Amazon SES:

```
aws ses list-identities
```

Output:

```
{
    "Identities": [
      "user@example.com",
      "example.com"
    ]
}
```

L'elenco restituito contiene tutte le identità indipendentemente dallo stato della verifica (verified, pending verification, failure, ecc.).

In questo esempio, gli indirizzi e-mail e i domini vengono restituiti perché non è stato specificato il parametro identity-type.

Per ulteriori informazioni riguardo alla verifica, consulta Verifica degli indirizzi e-mail e dei domini in Amazon SES nella Guida per gli sviluppatori di Amazon Simple Email Service.

- Per i dettagli sull'API, consulta AWS CLI Command ListIdentitiesReference.

Java

SDK per Java 2.x

> **Note**
>
> C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice 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);
        }
    }
}
```

- Per i dettagli sull'API, ListIdentitiesconsulta AWS SDK for Java 2.x API Reference.

JavaScript

SDK per JavaScript (v3)

> **Note**
>
> C'è altro da fare. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice 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;
  }
};
```

- Per i dettagli sull'API, ListIdentitiesconsulta AWS SDK for JavaScript API Reference.

PowerShell

Strumenti per PowerShell

Esempio 1: questo comando restituisce un elenco contenente tutte le identità (indirizzi e-mail e domini) per un AWS account specifico, indipendentemente dallo stato di verifica.

```
Get-SESIdentity
```

- Per i dettagli sull'API, vedere ListIdentitiesin AWS Tools for PowerShell Cmdlet Reference.

Python

SDK per Python (Boto3)

> **Note**
>
> C'è di più su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice 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
```

- Per i dettagli sull'API, consulta ListIdentities AWSSDK for Python (Boto3) API Reference.

Ruby

SDK per Ruby

> **Note**
>
> C'è di più su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice 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
```

- Per i dettagli sull'API, ListIdentitiesconsulta AWS SDK for Ruby API Reference.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consultaUtilizzo di Amazon SES con un AWS SDK. Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Utilizzo **`ListReceiptFilters`** con un AWS SDK o una CLI

I seguenti esempi di codice mostrano come utilizzare`ListReceiptFilters`.

C++

SDK per C++

> **Note**
>
> C'è altro su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice 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();
}
```

- Per i dettagli sull'API, ListReceiptFiltersconsulta AWS SDK for C++ API Reference.

JavaScript

SDK per JavaScript (v3)

> **Note**
>
> C'è altro da fare. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice 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);
};
```

- Per i dettagli sull'API, ListReceiptFiltersconsulta AWS SDK for JavaScript API Reference.

Python

SDK per Python (Boto3)

> **Note**
>
> C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice 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
```

- Per i dettagli sull'API, consulta ListReceiptFilters AWSSDK for Python (Boto3) API Reference.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. Utilizzo di Amazon SES con un AWS SDK Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Utilizzo **`ListTemplates`** con un AWS SDK o una CLI

I seguenti esempi di codice mostrano come utilizzare`ListTemplates`.

Gli esempi di operazioni sono estratti di codice da programmi più grandi e devono essere eseguiti nel contesto. È possibile visualizzare questa operazione nel contesto nel seguente esempio di codice:

- Verifica di un'identità e-mail e invio di messaggi

.NET

AWS SDK for .NET

> **Note**
>
> C'è altro su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice 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;
    }
```

- Per i dettagli sull'API, ListTemplatesconsulta AWS SDK for .NET API Reference.

Java

SDK per Java 2.x

> **Note**
>
> C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice 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);
        }
    }
}
```

- Per i dettagli sull'API, ListTemplatesconsulta AWS SDK for Java 2.x API Reference.

JavaScript

SDK per JavaScript (v3)

> **Note**
>
> C'è altro da fare. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice 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;
  }
};
```

- Per i dettagli sull'API, ListTemplatesconsulta AWS SDK for JavaScript API Reference.

Python

SDK per Python (Boto3)

> **Note**
>
> C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice 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
```

- Per i dettagli sull'API, consulta ListTemplates AWSSDK for Python (Boto3) API Reference.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. Utilizzo di Amazon SES con un AWS SDK Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Utilizzo **`SendBulkTemplatedEmail`** con un AWS SDK o una CLI

Il seguente esempio di codice mostra come utilizzare`SendBulkTemplatedEmail`.

JavaScript

SDK per JavaScript (v3)

> **Note**
>
> C'è altro da fare. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice 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;
  }
};
```

- Per i dettagli sull'API, SendBulkTemplatedEmailconsulta AWS SDK for JavaScript API Reference.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consultaUtilizzo di Amazon SES con un AWS SDK. Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Utilizzo **`SendEmail`** con un AWS SDK o una CLI

I seguenti esempi di codice mostrano come utilizzare`SendEmail`.

Gli esempi di operazioni sono estratti di codice da programmi più grandi e devono essere eseguiti nel contesto. È possibile visualizzare questa operazione nel contesto nel seguente esempio di codice:

- Verifica di un'identità e-mail e invio di messaggi

.NET

AWS SDK for .NET

> **Note**
>
> C'è altro su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice 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;
    }
```

- Per i dettagli sull'API, SendEmailconsulta AWS SDK for .NET API Reference.

C++

SDK per C++

> **Note**
>
> C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice 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();
}
```

- Per i dettagli sull'API, SendEmailconsulta AWS SDK for C++ API Reference.

CLI

AWS CLI

Invio di e-mail formattate utilizzando Amazon SES

Nell'esempio seguente viene utilizzato il comando `send-email` per inviare un messaggio e-mail formattato:

```
aws ses send-email --from sender@example.com --destination file://
destination.json --message file://message.json
```

Output:

```
{
   "MessageId": "EXAMPLEf3a5efcd1-51adec81-d2a4-4e3f-9fe2-5d85c1b23783-000000"
}
```

La destinazione e il messaggio sono strutture di dati JSON salvate in file .json nella directory corrente. Tali file sono i seguenti:

`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"
       }
   }
}
```

Sostituisci gli indirizzi e-mail del mittente e del destinatario con quelli che desideri utilizzare. Tieni presente che l'indirizzo e-mail del mittente deve essere verificato con Amazon SES. Fino a quando non ti viene concesso l'accesso alla produzione ad Amazon SES, devi verificare anche l'indirizzo e-mail di ciascun destinatario, a meno che il destinatario non sia il simulatore di mailbox Amazon SES. Per ulteriori informazioni riguardo alla verifica, consulta Verifica degli indirizzi e-mail e dei domini in Amazon SES nella Guida per gli sviluppatori di Amazon Simple Email Service.

L'ID del messaggio nell'output indica che la chiamata a send-email è stata completata correttamente.

Se non ricevi l'e-mail, controlla la casella della posta indesiderata.

Per ulteriori informazioni sull'invio di e-mail formattate, consulta Invio di e-mail formattate tramite l'API Amazon SES nella Guida per gli sviluppatori di Amazon Simple Email Service.

- Per i dettagli sull'API, consulta SendEmail AWS CLICommand Reference.

Java

SDK per Java 2.x

> **Note**
>
> C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice 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");
    }
}
```

- Per i dettagli sull'API, SendEmailconsulta AWS SDK for Java 2.x API Reference.

JavaScript

SDK per JavaScript (v3)

> **Note**
>
> C'è altro da fare. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice 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;
  }
};
```

- Per i dettagli sull'API, SendEmailconsulta AWS SDK for JavaScript API Reference.

Python

SDK per Python (Boto3)

> **Note**
>
> C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice 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
```

- Per i dettagli sull'API, consulta SendEmail AWSSDK for Python (Boto3) API Reference.

Ruby

SDK per Ruby

> **Note**
>
> C'è di più su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice 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
```

- Per i dettagli sull'API, SendEmailconsulta AWS SDK for Ruby API Reference.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consultaUtilizzo di Amazon SES con un AWS SDK. Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Utilizzo **`SendRawEmail`** con un AWS SDK o una CLI

I seguenti esempi di codice mostrano come utilizzare`SendRawEmail`.

CLI

AWS CLI

Invio di e-mail in formato RAW utilizzando Amazon SES

Nell'esempio seguente viene utilizzato il comando `send-raw-email` per inviare un messaggio con un allegato TXT:

```
aws ses send-raw-email --raw-message file://message.json
```

Output:

```
{
   "MessageId": "EXAMPLEf3f73d99b-c63fb06f-d263-41f8-a0fb-d0dc67d56c07-000000"
}
```

Il messaggio in formato RAW è una struttura di dati JSON salvata in un file denominato `message.json` nella directory corrente. Contiene i seguenti dati:

```
{
   "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--"
}
```

Come si vede, quella denominata "Data" è una lunga stringa con all'interno tutto il contenuto RAW dell'e-mail in formato MIME, incluso un allegato chiamato attachment.txt.

Sostituisci sender@example.com e recipient@example.com con gli indirizzi che desideri utilizzare. Tieni presente che l'indirizzo e-mail del mittente deve essere verificato con Amazon SES. Fino a quando non ti viene concesso l'accesso alla produzione ad Amazon SES, devi verificare anche l'indirizzo e-mail del destinatario, a meno che il destinatario non sia il simulatore di mailbox Amazon SES. Per ulteriori informazioni riguardo alla verifica, consulta Verifica degli indirizzi e-mail e dei domini in Amazon SES nella Guida per gli sviluppatori di Amazon Simple Email Service.

L'ID del messaggio nell'output indica che la chiamata a ha send-raw-email avuto esito positivo.

Se non ricevi l'e-mail, controlla la casella della posta indesiderata.

Per ulteriori informazioni sull'invio di e-mail in formato RAW, consulta Invio di e-mail in formato RAW tramite l'API Amazon SES nella Guida per gli sviluppatori di Amazon Simple Email Service.

- Per i dettagli sull'API, consulta SendRawEmail AWS CLICommand Reference.

JavaScript

SDK per JavaScript (v3)

> **Note**
>
> C'è altro da fare. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

Usare nodemailer per inviare un'e-mail con un allegato.

```
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);
        }
      },
    );
  });
};
```

- Per i dettagli sull'API, consulta la SendRawEmailsezione AWS SDK for JavaScript API Reference.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consultaUtilizzo di Amazon SES con un AWS SDK. Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Utilizzo **`SendTemplatedEmail`** con un AWS SDK o una CLI

I seguenti esempi di codice mostrano come utilizzare`SendTemplatedEmail`.

Gli esempi di operazioni sono estratti di codice da programmi più grandi e devono essere eseguiti nel contesto. È possibile visualizzare questa operazione nel contesto nel seguente esempio di codice:

- Verifica di un'identità e-mail e invio di messaggi

.NET

AWS SDK for .NET

> **Note**
>
> C'è altro su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice 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;
   }
```

- Per i dettagli sull'API, consulta la SendTemplatedEmailsezione AWS SDK for .NET API Reference.

C++

SDK per C++

> **Note**
>
> C'è di più su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
//! Send a templated email to a list of recipients.
/*!
  \param recipients; Vector of recipient email addresses.
  \param templateName: The name of the template to use.
  \param templateData: Map of key-value pairs for replacing text in template.
  \param senderEmailAddress: Email address of sender. Ignored if empty string.
  \param ccAddresses: Vector of cc addresses. Ignored if empty.
  \param replyToAddress: Reply to email address. Ignored if empty string.
  \param clientConfiguration: AWS client configuration.
  \return bool: Function succeeded.
 */
bool AwsDoc::SES::sendTemplatedEmail(const Aws::Vector<Aws::String> &recipients,
                                     const Aws::String &templateName,
                                     const Aws::Map<Aws::String, Aws::String>
 &templateData,
                                     const Aws::String &senderEmailAddress,
                                     const Aws::Vector<Aws::String> &ccAddresses,
                                     const Aws::String &replyToAddress,
                                     const Aws::Client::ClientConfiguration
 &clientConfiguration) {
    Aws::SES::SESClient sesClient(clientConfiguration);

    Aws::SES::Model::Destination destination;
    if (!ccAddresses.empty()) {
        destination.WithCcAddresses(ccAddresses);
    }
    if (!recipients.empty()) {
        destination.WithToAddresses(recipients);
```

```
    }

    Aws::SES::Model::SendTemplatedEmailRequest sendTemplatedEmailRequest;
    sendTemplatedEmailRequest.SetDestination(destination);
    sendTemplatedEmailRequest.SetTemplate(templateName);

    std::ostringstream templateDataStream;
    templateDataStream << "{";
    size_t dataCount = 0;
    for (auto &pair: templateData) {
        templateDataStream << "\"" << pair.first << "\":\"" << pair.second <<
 "\"";
        dataCount++;
        if (dataCount < templateData.size()) {
            templateDataStream << ",";
        }
    }
    templateDataStream << "}";

    sendTemplatedEmailRequest.SetTemplateData(templateDataStream.str());

    if (!senderEmailAddress.empty()) {
        sendTemplatedEmailRequest.SetSource(senderEmailAddress);
    }
    if (!replyToAddress.empty()) {
        sendTemplatedEmailRequest.AddReplyToAddresses(replyToAddress);
    }

    auto outcome = sesClient.SendTemplatedEmail(sendTemplatedEmailRequest);

    if (outcome.IsSuccess()) {
        std::cout << "Successfully sent templated message with ID "
                  << outcome.GetResult().GetMessageId()
                  << "." << std::endl;
    }
    else {
        std::cerr << "Error sending templated message. "
                  << outcome.GetError().GetMessage()
                  << std::endl;
    }

    return outcome.IsSuccess();
}
```

- Per i dettagli sull'API, consulta la SendTemplatedEmailsezione AWS SDK for C++ API Reference.

Java

SDK per Java 2.x

> **Note**
>
> C'è di più su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice 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);
        }
    }
}
```

- Per i dettagli sull'API, consulta la SendTemplatedEmailsezione AWS SDK for Java 2.x API Reference.

JavaScript

SDK per JavaScript (v3)

> **Note**
>
> C'è altro da fare. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice 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;
  }
};
```

- Per i dettagli sull'API, consulta la SendTemplatedEmailsezione AWS SDK for JavaScript API Reference.

Python

SDK per Python (Boto3)

> **Note**
>
> C'è di più su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice 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
```

- Per i dettagli sull'API, consulta SendTemplatedEmail AWSSDK for Python (Boto3) API Reference.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. Utilizzo di Amazon SES con un AWS SDK Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Utilizzo **`UpdateTemplate`** con un AWS SDK o una CLI

I seguenti esempi di codice mostrano come utilizzare`UpdateTemplate`.

Gli esempi di operazioni sono estratti di codice da programmi più grandi e devono essere eseguiti nel contesto. Puoi vedere questa azione nel contesto nel seguente esempio di codice:

- Verifica di un'identità e-mail e invio di messaggi

C++

SDK per C++

> **Note**
>
> C'è altro su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice 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();
}
```

- Per i dettagli sull'API, consulta la UpdateTemplatesezione AWS SDK for C++ API Reference.

JavaScript

SDK per JavaScript (v3)

> **Note**
>
> C'è altro da fare. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice 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;
  }
};
```

- Per i dettagli sull'API, consulta la UpdateTemplatesezione AWS SDK for JavaScript API Reference.

Python

SDK per Python (Boto3)

> **Note**
>
> C'è di più su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice 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
```

- Per i dettagli sull'API, consulta UpdateTemplate AWSSDK for Python (Boto3) API Reference.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. Utilizzo di Amazon SES con un AWS SDK Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Utilizzo **`VerifyDomainIdentity`** con un AWS SDK o una CLI

I seguenti esempi di codice mostrano come utilizzare`VerifyDomainIdentity`.

Gli esempi di operazioni sono estratti di codice da programmi più grandi e devono essere eseguiti nel contesto. È possibile visualizzare questa operazione nel contesto nei seguenti esempi di codice:

- Copia delle identità domini ed e-mail tra Regioni
- Verifica di un'identità e-mail e invio di messaggi

CLI

AWS CLI

Verifica di un dominio con Amazon SES

Nell'esempio seguente viene utilizzato il comando `verify-domain-identity` per verificare un dominio:

```
aws ses verify-domain-identity --domain example.com
```

Output:

```
{
   "VerificationToken": "eoEmxw+YaYhb3h3iVJHuXMJXqeu1q1/wwmvjuEXAMPLE"
}
```

Per completare la verifica del dominio, devi aggiungere un record TXT con il token di verifica restituito alle impostazioni DNS del tuo dominio. Per ulteriori informazioni, consulta Verifica dei domini nella Guida per gli sviluppatori di Amazon Simple Email Service.

- Per i dettagli sull'API, consulta VerifyDomainIdentity AWS CLICommand Reference.

JavaScript

SDK per JavaScript (v3)

> **Note**
>
> C'è altro da fare. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice 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;
  }
};
```

- Per i dettagli sull'API, consulta la VerifyDomainIdentitysezione AWS SDK for JavaScript API Reference.

Python

SDK per Python (Boto3)

> **Note**
>
> C'è di più su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice 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
```

- Per i dettagli sull'API, consulta VerifyDomainIdentity AWSSDK for Python (Boto3) API Reference.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. Utilizzo di Amazon SES con un AWS SDK Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Utilizzo **`VerifyEmailIdentity`** con un AWS SDK o una CLI

I seguenti esempi di codice mostrano come utilizzare`VerifyEmailIdentity`.

Gli esempi di operazioni sono estratti di codice da programmi più grandi e devono essere eseguiti nel contesto. È possibile visualizzare questa operazione nel contesto nei seguenti esempi di codice:

- Copia delle identità domini ed e-mail tra Regioni
- Verifica di un'identità e-mail e invio di messaggi

.NET

AWS SDK for .NET

> **Note**
>
> C'è altro su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice 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;
   }
```

- Per i dettagli sull'API, consulta la VerifyEmailIdentitysezione AWS SDK for .NET API Reference.

C++

SDK per C++

> **Note**
>
> C'è di più su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice 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();
}
```

- Per i dettagli sull'API, consulta la VerifyEmailIdentitysezione AWS SDK for C++ API Reference.

CLI

AWS CLI

Aggiungere e verificare un indirizzo e-mail con Amazon SES

Nell'esempio seguente viene utilizzato il comando `verify-email-identity` per verificare un indirizzo e-mail:

```
aws ses verify-email-identity --email-address user@example.com
```

Prima di poter inviare e-mail usando Amazon SES, è necessario verificare il dominio o l'indirizzo da cui si intende inviare l'e-mail per dimostrarne la proprietà. Se non disponi ancora dell'accesso alla produzione, devi verificare anche tutti gli indirizzi e-mail a cui invii messaggi, ad eccezione degli indirizzi e-mail forniti dal Simulatore di mailbox di Amazon SES.

Dopo verify-email-identity la chiamata, l'indirizzo e-mail riceverà un'e-mail di verifica. L'utente deve fare clic sul link nell'e-mail per completare il processo di verifica.

Per ulteriori informazioni, consulta Verifica degli indirizzi e-mail in Amazon SES nella Guida per gli sviluppatori di Amazon Simple Email Service.

- Per i dettagli sull'API, consulta VerifyEmailIdentity AWS CLICommand Reference.

JavaScript

SDK per JavaScript (v3)

> **Note**
>
> C'è altro da fare. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice 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;
  }
};
```

- Per i dettagli sull'API, consulta la VerifyEmailIdentitysezione AWS SDK for JavaScript API Reference.

Python

SDK per Python (Boto3)

> **Note**
>
> C'è di più su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice 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
```

- Per i dettagli sull'API, consulta VerifyEmailIdentity AWSSDK for Python (Boto3) API Reference.

Ruby

SDK per Ruby

> **Note**
>
> C'è di più su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice 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
```

- Per i dettagli sull'API, consulta la VerifyEmailIdentitysezione AWS SDK for Ruby API Reference.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consultaUtilizzo di Amazon SES con un AWS SDK. Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Scenari per Amazon SES che utilizzano AWS SDK

I seguenti esempi di codice mostrano come implementare scenari comuni in Amazon SES con AWS SDK. Questi scenari mostrano come eseguire attività specifiche richiamando più funzioni all'interno di Amazon SES. Ogni scenario include un collegamento a GitHub, dove puoi trovare istruzioni su come configurare ed eseguire il codice.

Esempi

- Copia le identità di e-mail e dominio di Amazon SES da una AWS regione all'altra utilizzando un SDK AWS
- Generazione di credenziali per eseguire la connessione a un endpoint SMTP di Amazon SES
- Verifica un'identità e-mail e invia messaggi con Amazon SES utilizzando un AWS SDK

Copia le identità di e-mail e dominio di Amazon SES da una AWS regione all'altra utilizzando un SDK AWS

Il seguente esempio di codice mostra come copiare le identità di e-mail e dominio di Amazon SES da una AWS regione all'altra. Quando le identità di dominio sono gestite da Route 53, i registri di verifica vengono copiati nel dominio della regione di destinazione.

Python

SDK per Python (Boto3)

> **Note**
>
> C'è altro su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice 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()
```

- Per informazioni dettagliate sull'API, consulta i seguenti argomenti nella Documentazione di riferimento delle API SDK AWS per Python (Boto3).
  - ListIdentities
  - SetIdentityNotificationTopic
  - VerifyDomainDkim
  - VerifyDomainIdentity
  - VerifyEmailIdentity

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consultaUtilizzo di Amazon SES con un AWS SDK. Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Generazione di credenziali per eseguire la connessione a un endpoint SMTP di Amazon SES

L'esempio di codice seguente mostra come generare credenziali per eseguire la connessione a un endpoint SMTP di Amazon SES.

Python

SDK per Python (Boto3)

> **Note**
>
> C'è altro su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice 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()
```

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consultaUtilizzo di Amazon SES con un AWS SDK. Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Verifica un'identità e-mail e invia messaggi con Amazon SES utilizzando un AWS SDK

L'esempio di codice seguente mostra come:

- Aggiungi e verifica un indirizzo e-mail con Amazon SES.
- Invia un messaggio di posta elettronica standard.
- Crea un modello e invia un messaggio e-mail basato sul modello.
- Invia un messaggio utilizzando un server SMTP di Amazon SES.

Python

SDK per Python (Boto3)

> **Note**
>
> C'è altro su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

Verifica un indirizzo e-mail con Amazon SES e invia i messaggi.

```
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)
```

Crea funzioni per includere le operazioni dell'identità 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
```

Crea funzioni per includere le operazioni del modello 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
```

Crea funzioni per includere le operazioni di posta elettronica di 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
```

- Per informazioni dettagliate sull'API, consulta i seguenti argomenti nella Documentazione di riferimento delle API SDK AWS per Python (Boto3).
  - CreateTemplate
  - DeleteIdentity
  - DeleteTemplate
  - GetIdentityVerificationAttributes
  - GetTemplate
  - ListIdentities
  - ListTemplates
  - SendEmail
  - SendTemplatedEmail
  - UpdateTemplate
  - VerifyDomainIdentity
  - VerifyEmailIdentity

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consultaUtilizzo di Amazon SES con un AWS SDK. Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Esempi di servizi multipli per Amazon SES che utilizzano SDK AWS

Le seguenti applicazioni di esempio utilizzano AWS gli SDK per combinare Amazon SES con altri Servizi AWS. Ogni esempio include un collegamento a GitHub, dove puoi trovare istruzioni su come configurare ed eseguire l'applicazione.

Esempi

- Creazione di un'app in streaming Amazon Transcribe
- Creazione di un'applicazione Web per tracciare i dati DynamoDB
- Come creare un tracker di articoli Amazon Redshift

- Creazione di un tracciatore di elementi di lavoro di Aurora Serverless
- Rileva i DPI nelle immagini con Amazon Rekognition utilizzando un SDK AWS
- Rileva oggetti nelle immagini con Amazon Rekognition utilizzando un SDK AWS
- Rileva persone e oggetti in un video con Amazon Rekognition utilizzando un SDK AWS
- Utilizzo di Step Functions per richiamare le funzioni Lambda

Creazione di un'app in streaming Amazon Transcribe

L'esempio di codice seguente mostra come creare un'applicazione che registra, trascrive e traduce l'audio in tempo reale e invia tramite e-mail i risultati.

JavaScript

SDK per JavaScript (v3)

Mostra come utilizzare Amazon Transcribe per creare un'applicazione che registra, trascrive e traduce l'audio in tempo reale e invia i risultati per e-mail tramite Amazon Simple Email Service (Amazon SES).

Per il codice sorgente completo e le istruzioni su come configurarlo ed eseguirlo, guarda l'esempio completo su. GitHub

Servizi utilizzati in questo esempio

- Amazon Comprehend
- Amazon SES
- Amazon Transcribe
- Amazon Translate

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consultaUtilizzo di Amazon SES con un AWS SDK. Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Creazione di un'applicazione Web per tracciare i dati DynamoDB

I seguenti esempi di codice mostrano come creare un'applicazione Web che traccia gli elementi di lavoro in una tabella Amazon DynamoDB e utilizza il Servizio di email semplice Amazon (Amazon SES) per inviare report.

.NET

AWS SDK for .NET

Mostra come utilizzare l'API Amazon DynamoDB per creare un'applicazione Web dinamica che traccia i dati di lavoro DynamoDB.

Per il codice sorgente completo e le istruzioni su come configurarlo ed eseguirlo, consulta l'esempio completo su GitHub.

Servizi utilizzati in questo esempio

- DynamoDB
- Amazon SES

Java

SDK per Java 2.x

Mostra come utilizzare l'API Amazon DynamoDB per creare un'applicazione Web dinamica che traccia i dati di lavoro DynamoDB.

Per il codice sorgente completo e le istruzioni su come configurarlo ed eseguirlo, guarda l'esempio completo su GitHub.

Servizi utilizzati in questo esempio

- DynamoDB
- Amazon SES

JavaScript

SDK per JavaScript (v3)

Mostra come utilizzare l'API Amazon DynamoDB per creare un'applicazione Web dinamica che traccia i dati di lavoro DynamoDB.

Per il codice sorgente completo e le istruzioni su come configurarlo ed eseguirlo, guarda l'esempio completo su. GitHub

Servizi utilizzati in questo esempio

- DynamoDB

- Amazon SES

Kotlin

SDK per Kotlin

Mostra come utilizzare l'API Amazon DynamoDB per creare un'applicazione Web dinamica che traccia i dati di lavoro DynamoDB.

Per il codice sorgente completo e le istruzioni su come configurarlo ed eseguirlo, guarda l'esempio completo su GitHub.

Servizi utilizzati in questo esempio

- DynamoDB
- Amazon SES

Python

SDK per Python (Boto3)

Mostra come utilizzare per AWS SDK for Python (Boto3) creare un servizio REST che tenga traccia degli elementi di lavoro in Amazon DynamoDB e invii report tramite e-mail utilizzando Amazon Simple Email Service (Amazon SES). Questo esempio utilizza il framework Web Flask per gestire il routing HTTP e si integra con una pagina Web React per presentare un'applicazione Web completamente funzionale.

- Crea un servizio Flask REST che si integri con. Servizi AWS
- Lettura, scrittura e aggiornamento di elementi di lavoro archiviati in una tabella DynamoDB.
- Utilizzo di Amazon SES per inviare report via e-mail sugli elementi di lavoro.

Per il codice sorgente completo e le istruzioni su come configurarlo ed eseguirlo, consulta l'esempio completo nel AWS Code Examples Repository su. GitHub

Servizi utilizzati in questo esempio

- DynamoDB
- Amazon SES

Per un elenco completo delle guide e degli esempi di codice per sviluppatori AWS SDK, consulta. Utilizzo di Amazon SES con un AWS SDK Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Come creare un tracker di articoli Amazon Redshift

Gli esempi di codice seguenti mostrano come creare un'applicazione Web che traccia e segnala gli elementi di lavoro tramite un database Amazon Redshift.

Java

SDK per Java 2.x

Mostra come creare un'applicazione Web che traccia e segnala gli elementi di lavoro archiviati in un database Amazon Redshift.

Per il codice sorgente completo e le istruzioni su come configurare un'API Spring REST che interroga i dati di Amazon Redshift e per l'utilizzo da parte di un'applicazione React, consulta l'esempio completo su. GitHub

Servizi utilizzati in questo esempio

- Amazon Redshift
- Amazon SES

Kotlin

SDK per Kotlin

Mostra come creare un'applicazione Web che traccia e segnala gli elementi di lavoro archiviati in un database Amazon Redshift.

Per il codice sorgente completo e le istruzioni su come configurare un'API Spring REST che interroga i dati di Amazon Redshift e per l'utilizzo da parte di un'applicazione React, consulta l'esempio completo su. GitHub

Servizi utilizzati in questo esempio

- Amazon Redshift
- Amazon SES

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. Utilizzo di Amazon SES con un AWS SDK Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Creazione di un tracciatore di elementi di lavoro di Aurora Serverless

I seguenti esempi di codice mostrano come creare un'applicazione Web che traccia gli elementi di lavoro in database Amazon Aurora Serverless e utilizza il Servizio di email semplice Amazon (Amazon SES) per inviare report.

.NET

AWS SDK for .NET

Mostra come utilizzare per AWS SDK for .NET creare un'applicazione Web che tenga traccia degli elementi di lavoro in un database Amazon Aurora e invii report tramite e-mail utilizzando Amazon Simple Email Service (Amazon SES). Questo esempio utilizza un front-end creato con React.js per interagire con un backend .NET RESTful.

- Integra un'applicazione web React con AWS i servizi.
- Elenco, aggiunta e aggiornamento di elementi in una tabella Aurora.
- Invia un report per e-mail degli articoli di lavoro filtrati tramite Amazon SES.
- Distribuisci e gestisci risorse di esempio con lo AWS CloudFormation script incluso.

Per il codice sorgente completo e le istruzioni su come configurarlo ed eseguirlo, vedi l'esempio completo su GitHub.

Servizi utilizzati in questo esempio

- Aurora
- Amazon RDS
- Servizi di dati di Amazon RDS
- Amazon SES

C++

SDK per C++

Mostra come creare un'applicazione Web che traccia gli elementi di lavoro archiviati in un database Amazon Aurora Serverless, con i relativi report.

Per il codice sorgente completo e le istruzioni su come configurare un'API REST C++ che interroga dati Amazon Aurora Serverless e per l'utilizzo da parte di un'applicazione React, consulta l'esempio completo su. GitHub

Servizi utilizzati in questo esempio

- Aurora
- Amazon RDS
- Servizi di dati di Amazon RDS
- Amazon SES

Java

SDK per Java 2.x

Mostra come creare un'applicazione Web che traccia e segnala gli elementi di lavoro archiviati in un database Amazon RDS.

Per il codice sorgente completo e le istruzioni su come configurare un'API Spring REST che interroga i dati Serverless di Amazon Aurora e per l'utilizzo da parte di un'applicazione React, consulta l'esempio completo su. GitHub

Per il codice sorgente completo e le istruzioni su come configurare ed eseguire un esempio che utilizza l'API JDBC, consulta l'esempio completo su. GitHub

Servizi utilizzati in questo esempio

- Aurora
- Amazon RDS
- Servizi di dati di Amazon RDS
- Amazon SES

JavaScript

SDK per (v3 JavaScript)

Mostra come utilizzare AWS SDK for JavaScript (v3) per creare un'applicazione Web che tenga traccia degli elementi di lavoro in un database Amazon Aurora e invii report tramite e-mail utilizzando Amazon Simple Email Service (Amazon SES). Questo esempio utilizza un front-end creato con React.js per interagire con un backend Express Node.js.

- Integra un'applicazione web React.js con. Servizi AWS
- Elenca, aggiungi e aggiorna elementi in una tabella Aurora.
- Invia un report per e-mail degli elementi di lavoro filtrati tramite Amazon SES.
- Distribuisci e gestisci risorse di esempio con lo AWS CloudFormation script incluso.

Per il codice sorgente completo e le istruzioni su come configurarlo ed eseguirlo, vedi l'esempio completo su GitHub.

Servizi utilizzati in questo esempio

- Aurora
- Amazon RDS
- Servizi di dati di Amazon RDS
- Amazon SES

Kotlin

SDK per Kotlin

Mostra come creare un'applicazione Web che traccia e segnala gli elementi di lavoro archiviati in un database Amazon RDS.

Per il codice sorgente completo e le istruzioni su come configurare un'API Spring REST che interroga i dati Serverless di Amazon Aurora e per l'utilizzo da parte di un'applicazione React, consulta l'esempio completo su. GitHub

Servizi utilizzati in questo esempio

- Aurora
- Amazon RDS
- Servizi di dati di Amazon RDS
- Amazon SES

PHP

SDK per PHP

Mostra come utilizzare per AWS SDK for PHP creare un'applicazione Web che tenga traccia degli elementi di lavoro in un database Amazon RDS e invii report tramite e-mail utilizzando

Amazon Simple Email Service (Amazon SES). Questo esempio utilizza un front-end creato con React.js per interagire con un backend PHP RESTful.

- Integra un'applicazione web React.js con AWS i servizi.
- Elenca, aggiungi, aggiorna ed elimina gli elementi in una tabella Amazon RDS.
- Invia un report per e-mail degli articoli di lavoro filtrati tramite Amazon SES.
- Distribuisci e gestisci risorse di esempio con lo AWS CloudFormation script incluso.

Per il codice sorgente completo e le istruzioni su come configurarlo ed eseguirlo, vedi l'esempio completo su GitHub.

Servizi utilizzati in questo esempio

- Aurora
- Amazon RDS
- Servizi di dati di Amazon RDS
- Amazon SES

Python

SDK per Python (Boto3)

Mostra come utilizzare per AWS SDK for Python (Boto3) creare un servizio REST che tenga traccia degli elementi di lavoro in un database Amazon Aurora Serverless e invii report tramite e-mail utilizzando Amazon Simple Email Service (Amazon SES). Questo esempio utilizza il framework Web Flask per gestire il routing HTTP e si integra con una pagina Web React per presentare un'applicazione Web completamente funzionale.

- Crea un servizio Flask REST che si integri con. Servizi AWS
- Lettura, scrittura e aggiornamento degli elementi di lavoro archiviati in un database Aurora Serverless.
- Crea un AWS Secrets Manager segreto che contenga le credenziali del database e usalo per autenticare le chiamate al database.
- Utilizzo di Amazon SES per inviare report via e-mail sugli elementi di lavoro.

Per il codice sorgente completo e le istruzioni su come configurarlo ed eseguirlo, guarda l'esempio completo su. GitHub

Servizi utilizzati in questo esempio

- Aurora
- Amazon RDS
- Servizi di dati di Amazon RDS
- Amazon SES

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consultaUtilizzo di Amazon SES con un AWS SDK. Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Rileva i DPI nelle immagini con Amazon Rekognition utilizzando un SDK AWS

Gli esempi di codice seguenti mostrano come creare un'applicazione che utilizza Amazon Rekognition per rilevare dispositivi di protezione individuale (DPI) nelle immagini.

Java

SDK per Java 2.x

Mostra come creare una AWS Lambda funzione che rileva le immagini con dispositivi di protezione individuale.

Per il codice sorgente completo e le istruzioni su come configurarlo ed eseguirlo, guarda l'esempio completo su GitHub.

Servizi utilizzati in questo esempio

- DynamoDB
- Amazon Rekognition
- Amazon S3
- Amazon SES

JavaScript

SDK per JavaScript (v3)

Mostra come usare Amazon Rekognition AWS SDK for JavaScript con la per creare un'applicazione per rilevare i dispositivi di protezione individuale (DPI) nelle immagini che si trovano in un bucket Amazon Simple Storage Service (Amazon S3). L'applicazione salva i

risultati in una tabella Amazon DynamoDB e invia all'amministratore una notifica e-mail sui risultati tramite Amazon Simple Email Service (Amazon SES).

Scopri come:

- Creare un utente non autenticato tramite Amazon Cognito.
- Analizzare le immagini per rilevare i DPI tramite Amazon Rekognition.
- Verificare un indirizzo e-mail per Amazon SES.
- Aggiornare una tabella DynamoDB con i risultati.
- Inviare una notifica e-mail tramite Amazon SES.

Per il codice sorgente completo e le istruzioni su come configurarlo ed eseguirlo, consulta l'esempio completo su. GitHub

Servizi utilizzati in questo esempio

- DynamoDB
- Amazon Rekognition
- Amazon S3
- Amazon SES

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consultaUtilizzo di Amazon SES con un AWS SDK. Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Rileva oggetti nelle immagini con Amazon Rekognition utilizzando un SDK AWS

Gli esempi di codice seguenti mostrano come creare un'applicazione che utilizza Amazon Rekognition per rilevare oggetti in base a una categoria nelle immagini.

.NET

AWS SDK for .NET

Mostra come utilizzare l'API .NET di Amazon Rekognition per creare un'applicazione che utilizza Amazon Rekognition per identificare gli oggetti in base a una categoria nelle immagini situate in un bucket Amazon Simple Storage Service (Amazon S3). L'applicazione invia all'amministratore una notifica e-mail sui risultati tramite Amazon Simple Email Service (Amazon SES).

Per il codice sorgente completo e le istruzioni su come configurarlo ed eseguirlo, consulta l'esempio completo su GitHub.

Servizi utilizzati in questo esempio

- Amazon Rekognition
- Amazon S3
- Amazon SES

Java

SDK per Java 2.x

Mostra come utilizzare l'API Java di Amazon Rekognition per creare un'applicazione che utilizza Amazon Rekognition per identificare gli oggetti in base a una categoria nelle immagini situate in un bucket Amazon Simple Storage Service (Amazon S3). L'applicazione invia all'amministratore una notifica e-mail sui risultati tramite Amazon Simple Email Service (Amazon SES).

Per il codice sorgente completo e le istruzioni su come configurarlo ed eseguirlo, guarda l'esempio completo su GitHub.

Servizi utilizzati in questo esempio

- Amazon Rekognition
- Amazon S3
- Amazon SES

JavaScript

SDK per JavaScript (v3)

Mostra come usare Amazon Rekognition AWS SDK for JavaScript con la per creare un'app che utilizzi Amazon Rekognition per identificare gli oggetti per categoria nelle immagini che si trovano in un bucket Amazon Simple Storage Service (Amazon S3). L'applicazione invia all'amministratore una notifica e-mail sui risultati tramite Amazon Simple Email Service (Amazon SES).

Scopri come:

- Creare un utente non autenticato tramite Amazon Cognito.
- Analizza le immagini per rilevare gli oggetti tramite Amazon Rekognition.
- Verificare un indirizzo e-mail per Amazon SES.
- Inviare una notifica e-mail tramite Amazon SES.

Per il codice sorgente completo e le istruzioni su come configurarlo ed eseguirlo, consulta l'esempio completo su. GitHub

Servizi utilizzati in questo esempio

- Amazon Rekognition
- Amazon S3
- Amazon SES

Kotlin

SDK per Kotlin

Mostra come utilizzare l'API Kotlin di Amazon Rekognition per creare un'applicazione che utilizza Amazon Rekognition per identificare gli oggetti in base a una categoria nelle immagini situate in un bucket Amazon Simple Storage Service (Amazon S3). L'applicazione invia all'amministratore una notifica e-mail sui risultati tramite Amazon Simple Email Service (Amazon SES).

Per il codice sorgente completo e le istruzioni su come configurarlo ed eseguirlo, guarda l'esempio completo su GitHub.

Servizi utilizzati in questo esempio

- Amazon Rekognition
- Amazon S3
- Amazon SES

Python

SDK per Python (Boto3)

Illustra come utilizzare il AWS SDK for Python (Boto3) per creare un'applicazione Web che consenta di eseguire le seguenti operazioni:

- Caricamento di foto in un bucket Amazon Simple Storage Service (Amazon S3).
- Utilizzo di Amazon Rekognition per analizzare ed etichettare le foto.
- Utilizzo di Amazon Simple Email Service (Amazon SES) per inviare report dell'analisi delle immagini tramite e-mail.

Questo esempio contiene due componenti principali: una pagina web scritta in JavaScript che è costruita con React e un servizio REST scritto in Python creato con Flask-RESTful.

È possibile utilizzare la pagina Web React per:

- Visualizzare un elenco di immagini archiviate nel bucket S3.
- Caricare le immagini dal computer nel bucket S3.
- Visualizzare immagini ed etichette che identificano gli elementi rilevati nell'immagine.
- Ottenere un report relativo a tutte le immagini nel bucket S3 e inviarlo tramite email.

La pagina Web richiama il servizio REST. Il servizio invia richieste a AWS per eseguire le seguenti operazioni:

- Ottenere e filtrare l'elenco delle immagini nel bucket S3.
- Caricare le foto nel bucket S3.
- Utilizzare Amazon Rekognition per analizzare le singole foto e ottenere un elenco di etichette che identificano gli articoli rilevati al loro interno.
- Analizzare tutte le foto presenti nel bucket S3 e usare Amazon SES per inviare un report tramite e-mail.

Per il codice sorgente completo e le istruzioni su come configurarlo ed eseguirlo, guarda l'esempio completo su. GitHub

Servizi utilizzati in questo esempio

- Amazon Rekognition
- Amazon S3
- Amazon SES

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consultaUtilizzo di Amazon SES con un AWS SDK. Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Rileva persone e oggetti in un video con Amazon Rekognition utilizzando un SDK AWS

Gli esempi di codice seguenti mostrano come rilevare persone e oggetti in un video con Amazon Rekognition.

Java

SDK per Java 2.x

Mostra come utilizzare l'API Java di Amazon Rekognition per creare un'applicazione che rileva volti e oggetti nei video situati in un bucket Amazon Simple Storage Service (Amazon S3). L'applicazione invia all'amministratore una notifica e-mail sui risultati tramite Amazon Simple Email Service (Amazon SES).

Per il codice sorgente completo e le istruzioni su come configurarlo ed eseguirlo, consulta l'esempio completo su GitHub.

Servizi utilizzati in questo esempio

- Amazon Rekognition
- Amazon S3
- Amazon SES

JavaScript

SDK per JavaScript (v3)

Mostra come usare Amazon Rekognition AWS SDK for JavaScript per creare un'app per rilevare volti e oggetti nei video che si trovano in un bucket Amazon Simple Storage Service (Amazon S3). L'applicazione invia all'amministratore una notifica e-mail sui risultati tramite Amazon Simple Email Service (Amazon SES).

Scopri come:

- Creare un utente non autenticato tramite Amazon Cognito.
- Analizzare le immagini per rilevare i DPI tramite Amazon Rekognition.
- Verificare un indirizzo e-mail per Amazon SES.
- Inviare una notifica e-mail tramite Amazon SES.

Per il codice sorgente completo e le istruzioni su come configurarlo ed eseguirlo, consulta l'esempio completo su. GitHub

Servizi utilizzati in questo esempio

- Amazon Rekognition
- Amazon S3
- Amazon SES

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consultaUtilizzo di Amazon SES con un AWS SDK. Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Utilizzo di Step Functions per richiamare le funzioni Lambda

I seguenti esempi di codice mostrano come creare una macchina a AWS Step Functions stati che richiama AWS Lambda funzioni in sequenza.

Java

SDK per Java 2.x

Mostra come creare un flusso di lavoro AWS serverless utilizzando AWS Step Functions and. AWS SDK for Java 2.x Ogni fase del flusso di lavoro viene implementata utilizzando una AWS Lambda funzione.

Per il codice sorgente completo e le istruzioni su come configurarlo ed eseguirlo, vedi l'esempio completo su GitHub.

Servizi utilizzati in questo esempio

- DynamoDB
- Lambda
- Amazon SES
- Step Functions

JavaScript

SDK per JavaScript (v3)

Mostra come creare un flusso di lavoro AWS serverless utilizzando AWS Step Functions and. AWS SDK for JavaScript Ogni fase del flusso di lavoro viene implementata utilizzando una AWS Lambda funzione.

Lambda è un servizio di calcolo che consente di eseguire il codice senza effettuare il provisioning o la gestione di server. Step Functions è un servizio di orchestrazione serverless che consente di combinare funzioni Lambda e altri servizi AWS per la creazione di applicazioni business-critical.

Per il codice sorgente completo e le istruzioni su come configurarlo ed eseguirlo, vedi l'esempio completo su GitHub.

Questo esempio è anche disponibile nella Guida per lo sviluppatore di AWS SDK for JavaScript v3 .

Servizi utilizzati in questo esempio

- DynamoDB
- Lambda
- Amazon SES
- Step Functions

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consultaUtilizzo di Amazon SES con un AWS SDK. Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Esempi di codice per Amazon SES API v2 con SDK AWS

I seguenti esempi di codice mostrano come utilizzare l'API Amazon SES v2 con un kit di sviluppo AWS software (SDK).

Le operazioni sono estratti di codice da programmi più grandi e devono essere eseguite nel contesto. Sebbene le operazioni mostrino come richiamare le singole funzioni del servizio, è possibile visualizzarle contestualizzate negli scenari correlati e negli esempi tra servizi.

Scenari: esempi di codice che mostrano come eseguire un'attività specifica richiamando più funzioni all'interno dello stesso servizio.

Per un elenco completo di guide ed esempi di codice per sviluppatori AWS SDK, consulta. Utilizzo di Amazon SES con un AWS SDK Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Esempi di codice

Azioni per Amazon SES API v2 tramite SDK AWS

I seguenti esempi di codice mostrano come eseguire singole azioni Amazon SES API v2 con gli AWS SDK. Questi estratti chiamano l'API Amazon SES v2 e sono estratti di codice da programmi più grandi che devono essere eseguiti in modo contestuale. Ogni esempio include un collegamento a GitHub, dove puoi trovare le istruzioni per la configurazione e l'esecuzione del codice.

Gli esempi seguenti includono solo le operazioni più comunemente utilizzate. Per un elenco completo, consulta la Documentazione di riferimento delle API Amazon Simple Email Service API v2.

Esempi

- Utilizzo GetEmailIdentity con un AWS SDK o una CLI
- Utilizzo ListContactLists con un AWS SDK o una CLI
- Utilizzo ListContacts con un AWS SDK o una CLI
- Utilizzo SendEmail con un AWS SDK o una CLI

Utilizzo **`CreateContact`** con un AWS SDK o una CLI

I seguenti esempi di codice mostrano come utilizzare`CreateContact`.

Gli esempi di operazioni sono estratti di codice da programmi più grandi e devono essere eseguiti nel contesto. È possibile visualizzare questa operazione nel contesto nel seguente esempio di codice:

- Workflow delle newsletter

.NET

AWS SDK for .NET

> **Note**
>
> C'è altro su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice 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;
    }
```

- Per i dettagli sull'API, consulta la CreateContactsezione AWS SDK for .NET API Reference.

Java

SDK per Java 2.x

> **Note**
>
> C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice 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;
     }
   }
```

- Per i dettagli sull'API, consulta la CreateContactsezione AWS SDK for Java 2.x API Reference.

Python

SDK per Python (Boto3)

> **Note**
>
> C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice 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
```

- Per i dettagli sull'API, consulta CreateContact AWSSDK for Python (Boto3) API Reference.

Rust

SDK per Rust

> **Note**
>
> C'è di più su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice 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(())
}
```

- Per i dettagli sulle API, consulta la CreateContactguida di riferimento all'API AWS SDK for Rust.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. Utilizzo di Amazon SES con un AWS SDK Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Utilizzo **`CreateContactList`** con un AWS SDK o una CLI

I seguenti esempi di codice mostrano come utilizzare`CreateContactList`.

Gli esempi di operazioni sono estratti di codice da programmi più grandi e devono essere eseguiti nel contesto. È possibile visualizzare questa operazione nel contesto nel seguente esempio di codice:

- Workflow delle newsletter

.NET

AWS SDK for .NET

> **Note**
>
> C'è altro su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice 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;
    }
```

- Per i dettagli sull'API, consulta la CreateContactListsezione AWS SDK for .NET API Reference.

Java

SDK per Java 2.x

> **Note**
>
> C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice 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;
    }
```

- Per i dettagli sull'API, consulta la CreateContactListsezione AWS SDK for Java 2.x API Reference.

Python

SDK per Python (Boto3)

> **Note**
>
> C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice 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
```

- Per i dettagli sull'API, consulta CreateContactList AWSSDK for Python (Boto3) API Reference.

Rust

SDK per Rust

> **Note**
>
> C'è di più su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice 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(())
}
```

- Per i dettagli sulle API, consulta la CreateContactListguida di riferimento all'API AWS SDK for Rust.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. Utilizzo di Amazon SES con un AWS SDK Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Utilizzo **`CreateEmailIdentity`** con un AWS SDK o una CLI

I seguenti esempi di codice mostrano come utilizzare`CreateEmailIdentity`.

Gli esempi di operazioni sono estratti di codice da programmi più grandi e devono essere eseguiti nel contesto. È possibile visualizzare questa operazione nel contesto nel seguente esempio di codice:

- Workflow delle newsletter

.NET

AWS SDK for .NET

> **Note**
>
> C'è altro su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice 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;
        }
    }
```

- Per i dettagli sull'API, consulta la CreateEmailIdentitysezione AWS SDK for .NET API Reference.

Java

SDK per Java 2.x

> **Note**
>
> C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice 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;
   }
```

- Per i dettagli sull'API, consulta la CreateEmailIdentitysezione AWS SDK for Java 2.x API Reference.

Python

SDK per Python (Boto3)

> **Note**
>
> C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice 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
```

- Per i dettagli sull'API, consulta CreateEmailIdentity AWSSDK for Python (Boto3) API Reference.

Rust

SDK per Rust

> **Note**
>
> C'è di più su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice 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)),
            },
```

```
        }
```

- Per i dettagli sulle API, consulta la CreateEmailIdentityguida di riferimento all'API AWS SDK for Rust.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. Utilizzo di Amazon SES con un AWS SDK Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Utilizzo **`CreateEmailTemplate`** con un AWS SDK o una CLI

I seguenti esempi di codice mostrano come utilizzare`CreateEmailTemplate`.

Gli esempi di operazioni sono estratti di codice da programmi più grandi e devono essere eseguiti nel contesto. È possibile visualizzare questa operazione nel contesto nel seguente esempio di codice:

- Workflow delle newsletter

.NET

AWS SDK for .NET

> **Note**
>
> C'è altro su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice 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;
    }
```

- Per i dettagli sull'API, consulta la CreateEmailTemplatesezione AWS SDK for .NET API Reference.

Java

SDK per Java 2.x

> **Note**
>
> C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice 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;
        }
```

- Per i dettagli sull'API, consulta la CreateEmailTemplatesezione AWS SDK for Java 2.x API Reference.

Python

SDK per Python (Boto3)

> **Note**
>
> C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice 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
```

- Per i dettagli sull'API, consulta CreateEmailTemplate AWSSDK for Python (Boto3) API Reference.

Rust

SDK per Rust

> **Note**
>
> C'è di più su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice 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)),
            },
        }
```

- Per i dettagli sulle API, consulta la CreateEmailTemplateguida di riferimento all'API AWS SDK for Rust.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. Utilizzo di Amazon SES con un AWS SDK Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Utilizzo **`DeleteContactList`** con un AWS SDK o una CLI

I seguenti esempi di codice mostrano come utilizzare`DeleteContactList`.

Gli esempi di operazioni sono estratti di codice da programmi più grandi e devono essere eseguiti nel contesto. È possibile visualizzare questa operazione nel contesto nel seguente esempio di codice:

- Workflow delle newsletter

.NET

AWS SDK for .NET

> **Note**
>
> C'è altro su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice 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;
    }
```

- Per i dettagli sull'API, consulta la DeleteContactListsezione AWS SDK for .NET API Reference.

Java

SDK per Java 2.x

> **Note**
>
> C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice 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();
    }
```

- Per i dettagli sull'API, consulta la DeleteContactListsezione AWS SDK for Java 2.x API Reference.

Python

SDK per Python (Boto3)

> **Note**
>
> C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice 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)
```

- Per i dettagli sull'API, consulta DeleteContactList AWSSDK for Python (Boto3) API Reference.

Rust

SDK per Rust

> **Note**
>
> C'è di più su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice 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}")),
        }
```

- Per i dettagli sulle API, consulta la DeleteContactListguida di riferimento all'API AWS SDK for Rust.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. Utilizzo di Amazon SES con un AWS SDK Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Utilizzo **`DeleteEmailIdentity`** con un AWS SDK o una CLI

I seguenti esempi di codice mostrano come utilizzare`DeleteEmailIdentity`.

Gli esempi di operazioni sono estratti di codice da programmi più grandi e devono essere eseguiti nel contesto. È possibile visualizzare questa operazione nel contesto nel seguente esempio di codice:

- Workflow delle newsletter

.NET

AWS SDK for .NET

> **Note**
>
> C'è altro su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice 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;
    }
```

- Per i dettagli sull'API, consulta la DeleteEmailIdentitysezione AWS SDK for .NET API Reference.

Java

SDK per Java 2.x

> **Note**
>
> C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice 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.");
        }
```

- Per i dettagli sull'API, consulta la DeleteEmailIdentitysezione AWS SDK for Java 2.x API Reference.

Python

SDK per Python (Boto3)

> **Note**
>
> C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice 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)
```

- Per i dettagli sull'API, consulta DeleteEmailIdentity AWSSDK for Python (Boto3) API Reference.

Rust

SDK per Rust

> **Note**
>
> C'è di più su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice 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));
                }
            }
```

- Per i dettagli sulle API, consulta la DeleteEmailIdentityguida di riferimento all'API AWS SDK for Rust.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. Utilizzo di Amazon SES con un AWS SDK Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Utilizzo **`DeleteEmailTemplate`** con un AWS SDK o una CLI

I seguenti esempi di codice mostrano come utilizzare`DeleteEmailTemplate`.

Gli esempi di operazioni sono estratti di codice da programmi più grandi e devono essere eseguiti nel contesto. È possibile visualizzare questa operazione nel contesto nel seguente esempio di codice:

- Workflow delle newsletter

.NET

AWS SDK for .NET

> **Note**
>
> C'è altro su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice 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;
    }
```

- Per i dettagli sull'API, consulta la DeleteEmailTemplatesezione AWS SDK for .NET API Reference.

Java

SDK per Java 2.x

> **Note**
>
> C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice 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();
   }
```

- Per i dettagli sull'API, consulta la DeleteEmailTemplatesezione AWS SDK for Java 2.x API Reference.

Python

SDK per Python (Boto3)

> **Note**
>
> C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice 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)
```

- Per i dettagli sull'API, consulta DeleteEmailTemplate AWSSDK for Python (Boto3) API Reference.

Rust

SDK per Rust

> **Note**
>
> C'è di più su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice 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}"));
            }
        }
```

- Per i dettagli sulle API, consulta la DeleteEmailTemplateguida di riferimento all'API AWS SDK for Rust.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. Utilizzo di Amazon SES con un AWS SDK Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Utilizzo **`GetEmailIdentity`** con un AWS SDK o una CLI

Il seguente esempio di codice mostra come utilizzare`GetEmailIdentity`.

Rust

SDK per Rust

> **Note**
>
> C'è altro su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

Determina se un indirizzo e-mail è stato verificato.

```
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(())
}
```

- Per i dettagli sulle API, consulta la GetEmailIdentityguida di riferimento all'API AWS SDK for Rust.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. Utilizzo di Amazon SES con un AWS SDK Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Utilizzo `ListContactLists` con un AWS SDK o una CLI

Il seguente esempio di codice mostra come utilizzare`ListContactLists`.

Rust

SDK per Rust

> **Note**
>
> C'è altro su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice 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(())
}
```

- Per i dettagli sulle API, consulta la ListContactListsguida di riferimento all'API AWS SDK for Rust.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. Utilizzo di Amazon SES con un AWS SDK Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Utilizzo `ListContacts` con un AWS SDK o una CLI

I seguenti esempi di codice mostrano come utilizzare`ListContacts`.

Gli esempi di operazioni sono estratti di codice da programmi più grandi e devono essere eseguiti nel contesto. È possibile visualizzare questa operazione nel contesto nel seguente esempio di codice:

- Workflow delle newsletter

.NET

AWS SDK for .NET

> **Note**
>
> C'è altro su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice 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>();
    }
```

- Per i dettagli sull'API, consulta la ListContactssezione AWS SDK for .NET API Reference.

Java

SDK per Java 2.x

> **Note**
>
> C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice 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;
     }
```

- Per i dettagli sull'API, consulta la ListContactssezione AWS SDK for Java 2.x API Reference.

Python

SDK per Python (Boto3)

> **Note**
>
> C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice 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
```

- Per i dettagli sull'API, consulta ListContacts AWSSDK for Python (Boto3) API Reference.

Rust

SDK per Rust

> **Note**
>
> C'è di più su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice 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(())
}
```

- Per i dettagli sulle API, consulta la ListContactsguida di riferimento all'API AWS SDK for Rust.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. Utilizzo di Amazon SES con un AWS SDK Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Utilizzo **`SendEmail`** con un AWS SDK o una CLI

I seguenti esempi di codice mostrano come utilizzare`SendEmail`.

.NET

AWS SDK for .NET

> **Note**
>
> C'è altro su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice 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;
    }
```

- Per i dettagli sull'API, consulta la SendEmailsezione AWS SDK for .NET API Reference.

Java

SDK per Java 2.x

> **Note**
>
> C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

Invio di un messaggio

```
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);
                }
        }
}
```

Invia un messaggio utilizzando un modello.

```
      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());
      }
```

- Per i dettagli sull'API, consulta la SendEmailsezione AWS SDK for Java 2.x API Reference.

Python

SDK per Python (Boto3)

> **Note**
>
> C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

Invia un messaggio a tutti i membri dell'elenco di contatti.

```
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}'.")
```

Invia un messaggio a tutti i membri dell'elenco dei contatti utilizzando un modello.

```
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},
                )
```

- Per i dettagli sull'API, consulta SendEmail AWSSDK for Python (Boto3) API Reference.

Ruby

SDK per Ruby

> **Note**
>
> C'è di più su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice 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)
```

- Per i dettagli sull'API, consulta la SendEmailsezione AWS SDK for Ruby API Reference.

Rust

SDK per Rust

> **Note**
>
> C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

Invia un messaggio a tutti i membri dell'elenco di contatti.

```
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(())
}
```

Invia un messaggio a tutti i membri dell'elenco dei contatti utilizzando un modello.

```
            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)),
            }
```

- Per i dettagli sull'API, consulta la SendEmailguida di riferimento all'API AWS SDK for Rust.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. Utilizzo di Amazon SES con un AWS SDK Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Scenari per Amazon SES API v2 con SDK AWS

I seguenti esempi di codice mostrano come implementare scenari comuni in Amazon SES API v2 con AWS SDK. Questi scenari mostrano come eseguire attività specifiche richiamando più funzioni all'interno dell'API Amazon SES v2. Ogni scenario include un collegamento a GitHub, dove puoi trovare istruzioni su come configurare ed eseguire il codice.

Esempi

- Un flusso di lavoro completo per la newsletter di Amazon SES API v2 utilizzando un SDK AWS

Un flusso di lavoro completo per la newsletter di Amazon SES API v2 utilizzando un SDK AWS

I seguenti esempi di codice mostrano come utilizzare il flusso di lavoro delle newsletter di Amazon SES API v2.

.NET

AWS SDK for .NET

> **Note**
>
> C'è altro su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

Esegui il flusso di lavoro.

```
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);
    }
}
```

Wrapper per le operazioni di assistenza.

```
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;
    }
}
```

- Per informazioni dettagliate sull'API, consulta i seguenti argomenti nella Documentazione di riferimento delle API AWS SDK for .NET .

- CreateContact
- CreateContactList
- CreateEmailIdentity
- CreateEmailTemplate
- DeleteContactList
- DeleteEmailIdentity
- DeleteEmailTemplate
- ListContacts
- SendEmail.semplice
- SendEmail.modello

Java

SDK per Java 2.x

> **Note**
>
> C'è altro da fare. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice 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();
    }
```

- Per informazioni dettagliate sull'API, consulta i seguenti argomenti nella Documentazione di riferimento delle API AWS SDK for Java 2.x .
  - CreateContact

- CreateContactList
- CreateEmailIdentity
- CreateEmailTemplate
- DeleteContactList
- DeleteEmailIdentity
- DeleteEmailTemplate
- ListContacts
- SendEmail.semplice
- SendEmail.modello

Python

SDK per Python (Boto3)

> **Note**
>
> C'è altro da fare. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice 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)
```

- Per informazioni dettagliate sull'API, consulta i seguenti argomenti nella Documentazione di riferimento delle API SDK AWS per Python (Boto3).
  - CreateContact
  - CreateContactList
  - CreateEmailIdentity
  - CreateEmailTemplate
  - DeleteContactList
  - DeleteEmailIdentity
  - DeleteEmailTemplate
  - ListContacts

- SendEmail.semplice
- SendEmail.modello

Rust

SDK per Rust

> **Note**
>
> C'è altro da fare. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice 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}"));
            }
        }
```

- Per informazioni dettagliate sulle API, consulta i seguenti argomenti nella Documentazione di riferimento delle API SDK AWS per Rust.
  - CreateContact

- CreateContactList
- CreateEmailIdentity
- CreateEmailTemplate
- DeleteContactList
- DeleteEmailIdentity
- DeleteEmailTemplate
- ListContacts
- SendEmail.semplice
- SendEmail.modello

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. Utilizzo di Amazon SES con un AWS SDK Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Sicurezza in Amazon Simple Email Service

La sicurezza del cloud AWS è la massima priorità. In qualità di AWS cliente, puoi beneficiare di un data center e di un'architettura di rete progettati per soddisfare i requisiti delle organizzazioni più sensibili alla sicurezza.

La sicurezza è una responsabilità condivisa tra AWS te e te. Il modello di responsabilità condivisa descrive questo modello come sicurezza del cloud e sicurezza nel cloud:

- Sicurezza del cloud: AWS è responsabile della protezione dell'infrastruttura che gestisce AWS i servizi nel AWS cloud. AWS ti fornisce anche servizi che puoi utilizzare in modo sicuro. I revisori esterni testano e verificano regolarmente l'efficacia della nostra sicurezza nell'ambito dei AWS Programmi di AWS conformità dei Programmi di conformità dei di . Per informazioni sui programmi di conformità che si applicano ad Amazon Simple Email Service, consulta AWS Services in Scope by Compliance Program AWS .
- Sicurezza nel cloud: la tua responsabilità è determinata dal AWS servizio che utilizzi. Sei anche responsabile di altri fattori, tra cui la riservatezza dei dati, i requisiti dell'azienda e le leggi e le normative applicabili.

Questa documentazione consente di comprendere come applicare il modello di responsabilità condivisa quando si usa Amazon Simple Email Service. Viene illustrato come configurare Amazon Simple Email Service per soddisfare gli obiettivi di sicurezza e conformità. Scopri anche come utilizzare altri AWS servizi che ti aiutano a monitorare e proteggere le tue risorse di Amazon Simple Email Service.

> **Note**
>
> Se devi segnalare un uso improprio delle AWS risorse, tra cui lo spam via e-mail e la distribuzione di malware, non utilizzare il link di feedback in nessuna delle pagine di questa guida per sviluppatori, poiché il modulo viene ricevuto dal team di AWS documentazione, non da AWS Trust & Safety. Invece, nella sezione Come posso segnalare un abuso di AWS risorse? pagina, segui le istruzioni per contattare il team AWS Trust & Safety per segnalare qualsiasi tipo di AWS abuso su Amazon.

Indice

Protezione dei dati in Amazon Simple Email Service

Il modello di responsabilità AWS condivisa modello si applica alla protezione dei dati in Amazon Simple Email Service. Come descritto in questo modello, AWS è responsabile della protezione dell'infrastruttura globale che gestisce tutti i Cloud AWS. L'utente è responsabile del controllo dei contenuti ospitati su questa infrastruttura. L'utente è inoltre responsabile della configurazione della protezione e delle attività di gestione per i Servizi AWS utilizzati. Per ulteriori informazioni sulla privacy dei dati, vedi le Domande frequenti sulla privacy dei dati. Per informazioni sulla protezione dei dati in Europa, consulta il post del blog relativo al Modello di responsabilità condivisa AWS e GDPR nel Blog sulla sicurezza AWS .

Ai fini della protezione dei dati, consigliamo di proteggere Account AWS le credenziali e configurare i singoli utenti con AWS IAM Identity Center or AWS Identity and Access Management (IAM). In tal modo, a ogni utente verranno assegnate solo le autorizzazioni necessarie per svolgere i suoi compiti. Ti suggeriamo, inoltre, di proteggere i dati nei seguenti modi:

- Utilizza l'autenticazione a più fattori (MFA) con ogni account.
- Usa SSL/TLS per comunicare con le risorse. AWS È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Configura l'API e la registrazione delle attività degli utenti con. AWS CloudTrail
- Utilizza soluzioni di AWS crittografia, insieme a tutti i controlli di sicurezza predefiniti all'interno Servizi AWS.
- Utilizza i servizi di sicurezza gestiti avanzati, come Amazon Macie, che aiutano a individuare e proteggere i dati sensibili archiviati in Amazon S3.
- Se hai bisogno di moduli crittografici convalidati FIPS 140-2 per l'accesso AWS tramite un'interfaccia a riga di comando o un'API, utilizza un endpoint FIPS. Per ulteriori informazioni sugli endpoint FIPS disponibili, consulta il Federal Information Processing Standard (FIPS) 140-2.

Ti consigliamo vivamente di non inserire mai informazioni riservate o sensibili, ad esempio gli indirizzi e-mail dei clienti, nei tag o nei campi di testo in formato libero, ad esempio nel campo Nome. Ciò include quando lavori con Amazon Simple Email Service o altro Servizi AWS utilizzando la console, l'API o AWS gli SDK. AWS CLI I dati inseriti nei tag o nei campi di testo in formato libero utilizzati per i nomi possono essere utilizzati per i la fatturazione o i log di diagnostica. Quando fornisci un URL a un server esterno, ti suggeriamo vivamente di non includere informazioni sulle credenziali nell'URL per convalidare la tua richiesta al server.

Indice

Crittografia dei dati a riposo per Amazon SES

Per impostazione predefinita, Amazon SES crittografa tutti i dati inattivi. La crittografia predefinita aiuta a ridurre il sovraccarico operativo e la complessità associati alla protezione dei dati. La crittografia consente inoltre di creare archivi di Mail Manager che soddisfano i rigorosi requisiti normativi e di conformità alla crittografia.

SES offre le seguenti opzioni di crittografia:

- AWS chiavi di proprietà: SES le utilizza per impostazione predefinita. Non è possibile visualizzare, gestire o utilizzare chiavi AWS di proprietà o controllarne l'utilizzo. Tuttavia, non è necessario effettuare alcuna operazione o modificare programmi per proteggere le chiavi che eseguono la crittografia dei dati. Per ulteriori informazioni, consulta la pagina chiavi di proprietàAWS nella Guida per gli sviluppatori di AWS Key Management Service .
- Chiavi gestite dal cliente: SES supporta l'uso di chiavi simmetriche gestite dal cliente che create, possedete e gestite. Poiché hai il pieno controllo della crittografia, puoi eseguire attività come:
  - Stabilire e mantenere le policy delle chiavi
  - Stabilire e mantenere le policy e le sovvenzioni IAM
  - Abilitare e disabilitare le policy delle chiavi
  - Ruotare i materiali crittografici delle chiavi
  - Aggiungere tag
  - Creare alias delle chiavi

- Pianificare l'eliminazione delle chiavi

Per utilizzare la tua chiave, scegli una chiave gestita dal cliente quando crei le tue risorse SES.

Per ulteriori informazioni, consulta Customer managed keys nella Guida per sviluppatori AWS Key Management Service .

> **Note**
>
> SES abilita automaticamente la crittografia a riposo utilizzando chiavi AWS di proprietà senza alcun costo.
> Tuttavia, l'utilizzo di una chiave gestita dal cliente comporta dei AWS KMS costi. Per ulteriori informazioni sui prezzi, consulta i AWS Key Management Service prezzi.

Creazione di una chiave gestita dal cliente

Puoi creare una chiave simmetrica gestita dal cliente utilizzando o AWS Management Console le AWS KMS API.

Per creare una chiave simmetrica gestita dal cliente

Segui i passaggi per la creazione di chiavi KMS di crittografia simmetrica nella Guida per gli sviluppatori.AWS Key Management Service

> **Note**
>
> Per l'archiviazione, la chiave deve soddisfare i seguenti requisiti:
>
> - La chiave deve essere simmetrica.
> - L'origine del materiale chiave deve essere. `AWS_KMS`
> - L'utilizzo della chiave deve essere`ENCRYPT_DECRYPT`.

Policy della chiave

Le policy della chiave controllano l'accesso alla chiave gestita dal cliente. Ogni chiave gestita dal cliente deve avere esattamente una policy della chiave, che contiene istruzioni che determinano

chi può usare la chiave e come la possono usare. Quando crei la chiave gestita dal cliente, puoi specificare una policy della chiave. Per ulteriori informazioni, consulta Gestione dell'accesso alle chiavi gestite dal cliente nella Guida per gli sviluppatori di AWS Key Management Service .

Per utilizzare la chiave gestita dal cliente con l'archiviazione di Mail Manager, la politica delle chiavi deve consentire le seguenti operazioni API:

- kms: DescribeKey — Fornisce i dettagli chiave gestiti dal cliente che consentono a SES di convalidare la chiave.
- kms: GenerateDataKey — Consente a SES di generare una chiave dati per crittografare i dati inattivi.
- kms:Decrypt — Consente a SES di decrittografare i dati memorizzati prima di restituirli ai client API.

L'esempio seguente mostra una politica chiave tipica:

```
{
            "Sid": "Allow SES to encrypt/decrypt",
            "Effect": "Allow",
            "Principal": {
                "Service": "ses.amazonaws.com"
            },
            "Action": [
                "kms:GenerateDataKey",
                "kms:Decrypt",
                "kms:DescribeKey"
            ],
            "Resource": "*"
        },
```

Per ulteriori informazioni, consulta Specificare le autorizzazioni in una politica, nella Guida per gli AWS Key Management Service sviluppatori.

Per ulteriori informazioni sulla risoluzione dei problemi, consulta la sezione Risoluzione dei problemi di accesso tramite chiave, nella Guida per gli AWS Key Management Service sviluppatori.

Specificazione di una chiave gestita dal cliente per l'archiviazione di Mail Manager

È possibile specificare una chiave gestita dal cliente come alternativa all'utilizzo di chiavi di AWS proprietà. Quando si crea un archivio, è possibile specificare la chiave dati inserendo una

chiave KMS ARN, che l'archiviazione di Mail Manager utilizza per crittografare tutti i dati dei clienti nell'archivio.

- ARN della chiave KMS: un identificatore chiave per AWS KMS una chiave gestita dal cliente. Inserisci l'ID della chiave, l'ARN della chiave, il nome dell'alias o l'ARN dell'alias.

Contesto di crittografia di Amazon SES

Un contesto di crittografia è un set facoltativo di coppie chiave-valore che contengono ulteriori informazioni contestuali sui dati.

AWS KMS utilizza il contesto di crittografia come dati autenticati aggiuntivi per supportare la crittografia autenticata. Quando includi un contesto di crittografia in una richiesta di crittografia dei dati, AWS KMS associa il contesto di crittografia ai dati crittografati. Per decrittografare i dati, nella richiesta deve essere incluso lo stesso contesto di crittografia.

> **Note**
>
> Amazon SES non supporta i contesti di crittografia per la creazione di archivi. Utilizza invece una policy IAM o KMS. Per esempioPolitiche di creazione degli archivi, consulta le politiche più avanti in questa sezione.

Contesto di crittografia Amazon SES

SES utilizza lo stesso contesto di crittografia in tutte le operazioni AWS KMS crittografiche, in cui la chiave è `aws:ses:arn` e il valore è la risorsa Amazon Resource Name (ARN).

Example

```
"encryptionContext": {
    "aws:ses:arn": "arn:aws:ses:us-west-2:111122223333:ExampleResourceName/
ExampleResourceID"
}
```

Utilizzo del contesto di crittografia per il monitoraggio

Quando utilizzi una chiave simmetrica gestita dal cliente per crittografare la tua risorsa SES, puoi anche utilizzare il contesto di crittografia nei record e nei log di controllo per identificare come viene

utilizzata la chiave gestita dal cliente. Il contesto di crittografia appare anche nei log generati da AWS CloudTrail o Amazon CloudWatch Logs.

Utilizzo del contesto di crittografia per controllare l'accesso alla chiave gestita dal cliente

È possibile utilizzare il contesto di crittografia nelle policy delle chiavi e nelle policy IAM come `conditions` per controllare l'accesso alla chiave simmetrica gestita dal cliente. È possibile utilizzare i vincoli del contesto di crittografia in una concessione.

SES utilizza un vincolo di contesto di crittografia nelle concessioni per controllare l'accesso alla chiave gestita dal cliente nell'account o nella regione dell'utente. Il vincolo della concessione richiede che le operazioni consentite dalla concessione utilizzino il contesto di crittografia specificato.

Example

Di seguito sono riportati alcuni esempi di istruzioni delle policy delle chiavi per concedere l'accesso a una chiave gestita dal cliente per un contesto di crittografia specifico. Questa istruzione della policy impone come condizione che le concessioni abbiano un vincolo che specifica il contesto di crittografia.

```
{
    "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"
          }
     }
```

```
}
```

Politiche di creazione degli archivi

Le seguenti politiche di esempio mostrano come abilitare la creazione di archivi. Le politiche funzionano su tutte le risorse.

Policy 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 policy

```
{
            "Sid": "Allow SES to encrypt/decrypt",
            "Effect": "Allow",
            "Principal": {
                "Service": "ses.amazonaws.com"
            },
            "Action": [
                "kms:GenerateDataKey",
```

```
                "kms:Decrypt",
                "kms:DescribeKey"
            ],
            "Resource": "*"
        },
```

Monitoraggio delle chiavi di crittografia per Amazon SES

Quando utilizzi una chiave gestita AWS KMS dal cliente con le tue risorse Amazon SES, puoi utilizzare AWS CloudTrailAmazon CloudWatch Logs per tenere traccia delle richieste inviate da AWS KMS SES.

Gli esempi seguenti sono AWS CloudTrail eventi per e per `GenerateDataKey` `DescribeKey` monitorare le operazioni KMS chiamate da SES per accedere ai dati crittografati dalla chiave gestita dal cliente: `Decrypt`

GenerateDataKey

Quando abiliti una chiave gestita AWS KMS dal cliente per la tua risorsa, SES crea una chiave di tabella unica. Invia una `GenerateDataKey` richiesta a AWS KMS che specifica la chiave gestita AWS KMS dal cliente per la risorsa.

Quando si abilita una chiave gestita AWS KMS dal cliente per la risorsa di archivio di Mail Manager, questa verrà utilizzata `GenerateDataKey` per crittografare i dati di archivio inattivi.

L'evento di esempio seguente registra l'operazione `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

Quando si accede a una risorsa crittografata, SES richiama l'`Decrypt`operazione per utilizzare la chiave dati crittografata memorizzata per accedere ai dati crittografati.

L'evento di esempio seguente registra l'operazione `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 utilizza l'`DescribeKey`operazione per verificare se la chiave gestita AWS KMS dal cliente associata alla risorsa esiste nell'account e nella regione.

L'evento di esempio seguente registra l'operazione `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"
}
```

Ulteriori informazioni

Le seguenti risorse forniscono ulteriori informazioni sulla crittografia dei dati a riposo.

- Per ulteriori informazioni su Concetti base di AWS Key Management Service, consulta la Guida per gli sviluppatori di AWS Key Management Service .
- Per ulteriori informazioni su Best Practice di sicurezza per AWS Key Management Service nella Guida per sviluppatori di AWS Key Management Service .

Crittografia in transito

Per impostazione predefinita, Amazon SES utilizza TLS opportunistico. Questo significa che Amazon SES tenta sempre di effettuare una connessione sicura al server di posta di ricezione. Se non è in grado di stabilire una connessione sicura, invia il messaggio non crittografato. Puoi modificare questo comportamento in modo che Amazon SES invii il messaggio al server e-mail di ricezione solo se è in grado di stabilire una connessione sicura. Per ulteriori informazioni, consulta Protocolli di sicurezza e Amazon SES.

Eliminazione di dati personali da Amazon SES

A seconda di come viene utilizzato, Amazon SES potrebbe archiviare determinati dati che potrebbero essere considerati personali. Ad esempio, per inviare e-mail usando Amazon SES, devi fornire almeno un'identità verificata (un indirizzo e-mail o un dominio). Puoi utilizzare la console Amazon SES o l'API Amazon SES per eliminare definitivamente questi dati personali.

Questo capitolo illustra le procedure per l'eliminazione di vari tipi di dati personali.

Indice

- Eliminazione di dati in modelli di e-mail di verifica personalizzati
- Elimina tutti i dati personali chiudendo l' AWS account

Eliminazione degli indirizzi e-mail dall'elenco di eliminazione a livello di account

Amazon SES include un elenco opzionale di eliminazione a livello di account. Quando si abilita questa caratteristica, gli indirizzi e-mail vengono automaticamente aggiunti a un elenco di eliminazione quando presentano un mancato recapito o un reclamo. Gli indirizzi e-mail rimangono in questo elenco fino a quando non vengono eliminati. Per ulteriori informazioni sull'elenco di eliminazione a livello di account, consulta Utilizzo dell'elenco di eliminazione a livello di account di Amazon SES.

È possibile rimuovere gli indirizzi e-mail dall'elenco di eliminazione a livello di account utilizzando l'operazione `DeleteSuppressedDestination` nell'API v2 Amazon SES. Questa sezione include una procedura per eliminare gli indirizzi e-mail utilizzando l' AWS CLI. Per ulteriori informazioni sull'installazione e la configurazione dell' AWS CLI, consulta la Guida per l'utente di AWS Command Line Interface.

Rimozione di un indirizzo dall'elenco di eliminazione a livello di account utilizzando l' AWS CLI

- Nella riga di comando, inserisci il comando seguente:

  ```
  aws sesv2 delete-suppressed-destination --email-address recipient@example.com
  ```

  Nel comando precedente sostituisci *recipient@example.com* con l'indirizzo e-mail che vuoi rimuovere dall'elenco di eliminazione a livello di account.

Eliminazione di dati relativi alle e-mail inviante mediante Amazon SES

Quando usi Amazon SES per inviare un'e-mail, puoi inviare informazioni su quell'e-mail ad altri AWS servizi. Ad esempio, è possibile inviare informazioni sugli eventi e-mail (come consegne, aperture e clic) a Firehose. In questo caso i dati contengono in genere il tuo indirizzo e-mail e l'indirizzo IP dal quale è stato inviato il messaggio e-mail. Tali dati contengono inoltre gli indirizzi e-mail di tutti i destinatari ai quali è stata inviata l'e-mail.

Puoi utilizzare Firehose per trasmettere i dati degli eventi e-mail verso diverse destinazioni, tra cui Amazon Simple Storage Service, Amazon Service e OpenSearch Amazon Redshift. Per rimuovere questi dati, è necessario prima interrompere lo streaming di dati su Firehose, quindi eliminare i

dati già trasmessi. Per interrompere lo streaming dei dati degli eventi Amazon SES su Firehose, è necessario eliminare la destinazione dell'evento Firehose.

Per rimuovere una destinazione di eventi Firehose utilizzando la console Amazon SES

1. Aprire la console di Amazon SES all'indirizzo https://console.aws.amazon.com/ses/.
2. In Email Sending (Invio e-mail), seleziona Configuration Sets (Set di configurazione).
3. Nell'elenco dei set di configurazione, scegliete il set di configurazione che contiene la destinazione dell'evento Firehose.
4. Accanto alla destinazione dell'evento Firehose che desiderate eliminare, scegliete il pulsante delete
   ( ).
5. Se necessario, rimuovere i dati che Firehose ha scritto su altri servizi. Per ulteriori informazioni, consulta the section called “Rimozione di dati relativi a eventi archiviati”.

Puoi utilizzare l'API Amazon SES per eliminare destinazioni di eventi. La procedura seguente utilizza AWS Command Line Interface (AWS CLI) per interagire con l'API Amazon SES. Puoi anche interagire con l'API utilizzando un AWS SDK o effettuando direttamente richieste HTTP.

Per rimuovere una destinazione di evento Firehose utilizzando il AWS CLI

1. Nella riga di comando, digita il comando seguente:

   ```
   aws sesv2 delete-configuration-set-event-destination --configuration-set-
   name configSet \
   --event-destination-name eventDestination
   ```

   In questo comando, sostituite *configSet* con il nome del set di configurazione che contiene la destinazione dell'evento Firehose. Sostituite *EventDestination* con il nome della destinazione dell'evento Firehose.
2. Se necessario, rimuovere i dati che Firehose ha scritto su altri servizi. Per ulteriori informazioni, consulta the section called “Rimozione di dati relativi a eventi archiviati”.

Rimozione di dati relativi a eventi archiviati

Per ulteriori informazioni sull'eliminazione di informazioni da altri AWS servizi, consultate i seguenti documenti:

- Eliminazione di un oggetto e un bucket nella Guida per l'utente di Amazon Simple Storage Service
- Eliminare un dominio OpenSearch di servizio nella Amazon OpenSearch Service Developer Guide
- Eliminazione di un cluster nella Guida alla gestione dei cluster di Amazon Redshift

Puoi anche utilizzare Firehose per trasmettere dati e-mail a Splunk, un servizio di terze parti che non è supportato AWS o gestito in. AWS Management Console Per ulteriori informazioni sulla rimozione di dati da Splunk, consulta l'amministratore di sistema o la documentazione presente sul Sito Web Splunk.

Eliminazione di dati relativi alle identità

Le identità includono gli indirizzi e-mail e i domini che puoi impiegare per inviare e-mail utilizzando Amazon SES. In alcune giurisdizioni, domini o indirizzi e-mail potrebbe essere considerati dati di identificazione personale.

Per eliminare un'identità utilizzando la console di Amazon SES

1. Aprire la console di Amazon SES all'indirizzo https://console.aws.amazon.com/ses/.
2. In Identity Management (Gestione identità), procedi in uno dei seguenti modi:
   - Scegli Domains (Domini) se desideri eliminare un dominio.
   - Seleziona Email Addresses (Indirizzi e-mail) se desideri eliminare un indirizzo e-mail.
3. Seleziona l'identità che desideri eliminare e quindi seleziona Remove (Rimuovi).
4. Nella finestra di dialogo di conferma, scegliere Yes, Delete Identity (Sì, elimina identità).

Puoi utilizzare l'operazione API Amazon SES per eliminare identità. La procedura seguente usa AWS Command Line Interface (AWS CLI) per l'interazione con l'API Amazon SES. Puoi anche interagire con l'API utilizzando un AWS SDK o effettuando direttamente richieste HTTP.

Per eliminare un'identità utilizzando il AWS CLI

- Nella riga di comando, digita il comando seguente:

```
aws ses delete-identity --identity sender@example.com
```

  In questo comando, sostituisci *sender@example.com* con l'identità che desideri eliminare.

Eliminazione di dati di autenticazione del mittente

L'autenticazione del mittente permette di controllare il processo di configurazione di Amazon SES in modo che un altro utente possa inviare e-mail a tuo nome. Per abilitare l'autorizzazione del mittente, devi creare una policy, come descritto in Uso dell'autorizzazione di invio con Amazon SES. Queste politiche contengono identità (che appartengono all'utente), oltre agli AWS ID (associati alla persona o al gruppo che invia e-mail per conto dell'utente). Puoi rimuovere questi dati personali modificando o eliminando le policy di autenticazione del mittente. Le procedure seguenti mostrano come eliminare queste policy.

Per eliminare una policy di autenticazione del mittente utilizzando la console di Amazon SES

1. Aprire la console di Amazon SES all'indirizzo https://console.aws.amazon.com/ses/.
2. In Identity Management (Gestione identità), procedi in uno dei seguenti modi:
   - Scegli Domains (Domini) se la policy di autenticazione del mittente da eliminare è associata a un dominio.
   - Scegli Email Addresses (Indirizzi e-mail) se la policy di autenticazione del mittente da eliminare è associata a un indirizzo e-mail.
3. In Identity Policies (Policy di identità), seleziona la policy che desideri eliminare e quindi seleziona Remove Policy (Elimina policy).

Puoi utilizzare l'operazione API Amazon SES per eliminare policy di autenticazione del mittente. La procedura seguente utilizza AWS Command Line Interface (AWS CLI) per interagire con l'API Amazon SES. Puoi anche interagire con l'API utilizzando un AWS SDK o effettuando direttamente richieste HTTP.

Per eliminare una politica di autenticazione del mittente utilizzando il AWS CLI

- Nella riga di comando, digita il comando seguente:

```
aws ses delete-identity-policy --identity example.com --policy-name samplePolicy
```

  In questo comando, sostituisci *example.com* con l'identità contenente la policy di autenticazione del mittente. Sostituisci *samplePolicy* con il nome della policy di autenticazione del mittente.

Eliminazione di dati relativi alle regole di ricezione

Se utilizzi Amazon SES per ricevere e-mail in ingresso, puoi creare regole di ricezione che vengono applicate a una o più identità (indirizzi e-mail o domini). Tali regole stabiliscono le operazioni effettuate da Amazon SES con la posta in arrivo inviata alle identità specificate.

Per eliminare una regola di ricezione utilizzando la console di Amazon SES

1. Aprire la console di Amazon SES all'indirizzo https://console.aws.amazon.com/ses/.
2. In Email Receiving (Ricezione e-mail), scegli Rule Sets (Set di regole).
3. Se la regola di ricezione fa parte del set di regole attive, scegli View Active Rule Set (Visualizza set di regole attive). In caso contrario, scegli il set di regole che contiene la regola di ricezione che desideri eliminare.
4. Nell'elenco delle regole di ricezione, seleziona la regola che desideri eliminare.
5. Dal menu Actions (Operazioni), scegli Delete (Elimina).
6. Nella finestra di dialogo di conferma, seleziona Delete (Elimina).

Puoi utilizzare l'operazione API Amazon SES per eliminare le regole di ricezione. La procedura seguente utilizza AWS Command Line Interface (AWS CLI) per interagire con l'API Amazon SES. Puoi anche interagire con l'API utilizzando un AWS SDK o effettuando direttamente richieste HTTP.

Per eliminare una regola di ricezione utilizzando il AWS CLI

- Nella riga di comando, digita il comando seguente:

```
aws ses delete-receipt-rule --rule-set myRuleSet --rule-name myReceiptRule
```

  In questo comando, sostituiscila *myRuleSet*con il nome del set di regole di incasso che contiene la regola di incasso. Sostituisci *myReceiptRule*con il nome della regola di incasso che desideri eliminare.

Eliminazione di dati relativi ai filtri di indirizzi IP

Se utilizzi Amazon SES per ricevere e-mail in ingresso, puoi creare filtri per accettare o bloccare esplicitamente dei messaggi inviati da indirizzi IP specifici.

Per rimuovere un filtro di indirizzi IP usando la console di Amazon SES

1. Aprire la console di Amazon SES all'indirizzo https://console.aws.amazon.com/ses/.
2. In Email Receiving (Ricezione e-mail), seleziona IP Address Filters (Filtri di indirizzi IP).
3. Nell'elenco di filtri di indirizzi IP, seleziona il filtro che desideri rimuovere e quindi scegli Delete (Elimina).

Puoi inoltre utilizzare l'operazione API Amazon SES per eliminare filtri di indirizzi IP. La procedura seguente utilizza AWS Command Line Interface (AWS CLI) per interagire con l'API Amazon SES. Puoi anche interagire con l'API utilizzando un AWS SDK o effettuando direttamente richieste HTTP.

Per eliminare un filtro di indirizzi IP utilizzando il AWS CLI

- Nella riga di comando, digita il comando seguente:

```
aws ses delete-receipt-filter --filter-name IPfilter
```

  In questo comando, sostituisci *IPfilter* con il nome del filtro di indirizzi IP che vuoi eliminare.

Eliminazione di dati in modelli di e-mail

Se utilizzi dei modelli di e-mail per l'invio di e-mail, è possibile che questi modelli contengano informazioni personali, a seconda di come il modello è stato configurato. Ad esempio, è possibile che sia stato aggiunto al modello un indirizzo e-mail che i destinatari possono contattare per ulteriori informazioni.

Puoi eliminare dei modelli di e-mail solo utilizzando l'API Amazon SES.

Per eliminare un modello di e-mail utilizzando il AWS CLI

- Nella riga di comando, digita il comando seguente:

```
aws ses delete-template --template-name sampleTemplate
```

  In questo comando, sostituisci *sampleTemplate* con il nome del modello di e-mail che vuoi eliminare.

Eliminazione di dati in modelli di e-mail di verifica personalizzati

Se utilizzi dei modelli di e-mail personalizzati per verificare i nuovi indirizzi di invio delle e-mail, è possibile che questi modelli contengano informazioni personali, a seconda di come il modello è stato configurato. Ad esempio, è possibile che sia stato aggiunto al modello di e-mail di verifica un indirizzo e-mail che i destinatari possono contattare per ulteriori informazioni.

Puoi eliminare dei modelli di e-mail di verifica personalizzati solo utilizzando l'API Amazon SES.

Per eliminare un modello di email di verifica personalizzato utilizzando il AWS CLI

- Nella riga di comando, digita il comando seguente:

  ```
  aws ses delete-custom-verification-email-template --template-
  name verificationEmailTemplate
  ```

  In questo comando, sostituiscilo *verificationEmailTemplate*con il nome del modello di email di verifica personalizzato che desideri eliminare.

Elimina tutti i dati personali chiudendo l' AWS account

Puoi inoltre eliminare tutti i dati personali memorizzati in Amazon SES chiudendo il tuo account AWS . Tuttavia, questa azione elimina anche tutti gli altri dati, personali o non personali, archiviati in ogni altro servizio. AWS

Quando chiudi l' AWS account, i dati in esso contenuti vengono conservati per 90 giorni. AWS Trascorso il periodo di conservazione, tali dati vengono eliminati in modo definitivo e irreversibile.

Per chiudere il tuo account AWS

Le istruzioni complete su come chiudere l' AWS account sono riportate in Chiudere un AWS account.

Identity and Access Management in Amazon SES

Puoi utilizzare AWS Identity and Access Management (IAM) con Amazon Simple Email Service (Amazon SES) per specificare quali azioni API SES possono eseguire un utente, un gruppo o un ruolo. In questo argomento queste entità vengono indicate collettivamente con il termine utente. Puoi anche determinare quali indirizzi e-mail possono essere utilizzati dall'utente per gli indirizzi "From", "To" e "Return-Path" delle e-mail.

Ad esempio, puoi creare una policy IAM che consente agli utenti nell'organizzazione di inviare e-mail ma non di eseguire operazioni amministrative, come controllare le statistiche di invio. Come altro esempio, puoi scrivere una policy che consente a un utente di inviare e-mail tramite SES dal tuo account, ma solo se utilizza un determinato indirizzo "From".

Per utilizzare IAM, devi definire una policy IAM, ossia un documento che definisce in modo esplicito le autorizzazioni, e collegare la policy a un utente. Per informazioni su come creare policy IAM, consulta la Guida per l'utente IAM. Salvo per l'applicazione delle limitazioni impostate nella policy, non ci sono variazioni nelle modalità con cui gli utenti interagiscono con SES o con cui SES esegue le richieste.

> **Note**
>
> - Se il tuo account è ancora nella sandbox SES, le sue restrizioni impediscono l'implementazione di alcune di queste policy - vedi Richiesta dell'accesso di produzione.
> - Puoi inoltre controllare l'accesso a SES utilizzando policy di autorizzazione all'invio. Mentre le policy IAM limitano le operazioni dei singoli utenti, le policy di autorizzazione di invio limitano il modo in cui le singole identità verificate possono essere utilizzate. Inoltre, solo le policy di autorizzazione all'invio possono concedere l'accesso multiaccount. Per ulteriori informazioni sull'autorizzazione all'invio, consulta Uso dell'autorizzazione di invio con Amazon SES.

Se cerchi informazioni su come generare le credenziali SMTP SES per un utente esistente, consulta Richiesta delle credenziali SMTP Amazon SES.

Creazione di policy IAM per l'accesso a SES

Questa sezione spiega in che modo puoi utilizzare le policy IAM specificamente con SES. Per informazioni su come creare policy IAM in generale, consulta la Guida per l'utente IAM.

Esistono tre possibili motivi per utilizzare IAM con SES:

- per limitare l'operazione di invio di e-mail;
- per limitare gli indirizzi "From", "To" e "Return-Path" delle e-mail che l'utente invia;
- per controllare gli aspetti generali di utilizzo delle API, ad esempio il periodo di tempo durante il quale un utente può chiamare le API che è autorizzato a utilizzare.

Limitazione delle operazioni

Per determinare quali operazioni SES possono essere eseguite da un utente, devi utilizzare l'elemento `Action` di una policy IAM. Puoi impostare l'elemento `Action` su qualsiasi operazione dell'API SES anteponendo al nome dell'API la stringa minuscola `ses:` come prefisso. Ad esempio, puoi impostare `Action` su `ses:SendEmail`, `ses:GetSendStatistics` o `ses:*` (per tutte le operazioni).

Quindi, a seconda di `Action`, specifica l'elemento `Resource` come segue:

Se l'elemento **`Action`** consente l'accesso solo alle API di invio di e-mail (cioè **`ses:SendEmail`** e/o **`ses:SendRawEmail`**):

- Per consentire all'utente di inviare messaggi da qualsiasi identità del tuo account Account AWS, imposta `Resource` su*
- Per limitare le identità da cui un utente può inviare, imposta `Resource` sugli ARN delle identità che stai permettendo all'utente di utilizzare.

Se l'elemento **`Action`** consente l'accesso a tutte le API:

- Se non vuoi limitare le identità da cui l'utente può inviare, imposta `Resource` su *.
- Se desideri limitare le identità da cui un utente può inviare, è necessario creare due policy (o due istruzioni all'interno di una policy):
  - Uno `Action` impostato su un elenco esplicito delle non-email-sending API consentite e `Resource` impostato su*
  - una in cui `Action` è impostato su una delle API di invio di e-mail (`ses:SendEmail` e/o `ses:SendRawEmail`) e `Resource` è impostato sugli ARN delle identità il cui uso vuoi consentire all'utente.

Per un elenco delle operazioni di Amazon SES disponibili, consulta la Documentazione di riferimento dell'API Amazon Simple Email Service. Se l'utente utilizzerà l'interfaccia SMTP, devi consentire l'accesso almeno a `ses:SendRawEmail`.

Limitazione degli indirizzi e-mail

Se desideri limitare l'utente a specifici indirizzi e-mail, puoi utilizzare un blocco `Condition`. Nel blocco `Condition` devi specificare le condizioni utilizzando chiavi di condizione come descritto nella Guida per l'utente IAM. Le chiavi di condizione consentono di controllare i seguenti indirizzi e-mail:

> **Note**
>
> Queste chiavi di condizione per indirizzi e-mail sono valide solo per le API indicate nella seguente tabella.

Chiave di condizione	Descrizione	API
`ses:Recipients`	Limita gli indirizzi del destinatario, che includono gli indirizzi "A", "CC" e "CCN".	`SendEmail` , `SendRawEmail`
`ses:FromAddress`	Limita l'indirizzo "From".	`SendEmail` , `SendRawEmail` , `SendBounce`
`ses:FromDisplayName`	Limita l'indirizzo "From" che viene utilizzato come nome visualizzato.	`SendEmail` , `SendRawEmail`
`ses:FeedbackAddress`	Limita l'indirizzo "Return-Path", che è l'indirizzo a cui mancati recapiti e reclami ti possono essere inviati tramite l'inoltro di feedback via e-mail. Per informazioni sull'inoltro di feedback via e-mail, consulta Ricezione delle notifiche Amazon SES tramite e-mail.	`SendEmail` , `SendRawEmail`

Limitazione per versione API SES

Usando la chiave `ses:ApiVersion` in condizioni, è possibile limitare l'accesso a SES in base alla versione dell'API SES.

> **Note**
>
> L'interfaccia SMTP SES utilizza l’API SES versione 2 di `ses:SendRawEmail`.

Limitazione dell'utilizzo generale delle API

Utilizzando le chiavi AWS-wide in determinate condizioni, è possibile limitare l'accesso a SES in base ad aspetti quali la data e l'ora in cui l'utente può accedere alle API. SES implementa solo le seguenti chiavi di policy a livello di AWS estensione:

- `aws:CurrentTime`
- `aws:EpochTime`
- `aws:SecureTransport`
- `aws:SourceIp`
- `aws:SourceVpc`
- `aws:SourceVpce`
- `aws:UserAgent`
- `aws:VpcSourceIp`

Per ulteriori informazioni su queste chiavi, consulta la Guida per l'utente IAM.

Esempi di policy IAM per SES

Questo argomento fornisce esempi di policy che consentono a un utente di accedere a SES, ma solo a determinate condizioni.

Esempi di policy riportati in questa sezione:

- Impostazione dell'accesso completo a tutte le operazioni SES
- Consentire l'accesso solo alle API SES versione 2
- Impostazione dell'accesso solo a operazioni di invio di e-mail
- Limitazione del periodo di tempo di invio
- Limitazione degli indirizzi del destinatario
- Limitazione dell'indirizzo "From"
- Limitazione del nome visualizzato del mittente dell'e-mail
- Limitazione della destinazione del feedback su mancato recapito e reclamo

Impostazione dell'accesso completo a tutte le operazioni SES

La policy seguente permette a un utente di chiamare qualsiasi operazione SES.

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

Consentire l'accesso solo alle API SES versione 2

La policy seguente permette a un utente di chiamare solo le operazioni SES dell'API versione 2.

```
{
                    "Version":"2012-10-17",
                    "Statement":[
                        {
                            "Effect":"Allow",
                            "Action":[
                            "ses:*"
                            ],
                            "Resource":"*",
                            "Condition": {
                                "StringEquals" : {
                                "ses:ApiVersion" : "2"
                                }
                            }
                        }
                    ]
                }
```

Impostazione dell'accesso solo a operazioni di invio di e-mail

La policy seguente consente a un utente di inviare e-mail utilizzando SES, ma non di eseguire altre operazioni di livello amministrativo, ad esempio accedere alle statistiche di invio SES.

```
{
```

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

Limitazione del periodo di tempo di invio

La policy seguente consente a un utente di chiamare le API di invio di e-mail SES soltanto durante il mese di settembre 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"
        }
      }
    }
  ]
}
```

Limitazione degli indirizzi del destinatario

La policy seguente consente a un utente di richiamare le API di invio di e-mail SES, ma solo per gli indirizzi dei destinatari nel dominio example.com (`StringLike` fa distinzione tra maiuscole e minuscole).

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Action":[
        "ses:SendEmail",
        "ses:SendRawEmail"
      ],
      "Resource":"*",
      "Condition":{
        "ForAllValues:StringLike":{
          "ses:Recipients":[
            "*@example.com"
          ]
        }
      }
    }
  ]
}
```

Limitazione dell'indirizzo "From"

La policy seguente consente a un utente di chiamare le API di invio di e-mail SES, ma solo se l'indirizzo "From" è marketing@example.com.

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

```
      "Condition":{
        "StringEquals":{
          "ses:FromAddress":"marketing@example.com"
        }
      }
    }
  ]
}
```

La seguente politica consente a un utente di chiamare l'SendBounceAPI, ma solo se l'indirizzo «Da» è bounce@example.com.

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Action":[
        "ses:SendBounce"
      ],
      "Resource":"*",
      "Condition":{
        "StringEquals":{
          "ses:FromAddress":"bounce@example.com"
        }
      }
    }
  ]
}
```

Limitazione del nome visualizzato del mittente dell'e-mail

La policy seguente consente a un utente di richiamare le API di invio di e-mail SES, ma solo se il nome visualizzato dell'indirizzo "From" include Marketing (`StringLike` fa distinzione tra maiuscole e minuscole).

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Action":[
```

```
        "ses:SendEmail",
        "ses:SendRawEmail"
      ],
      "Resource":"*",
      "Condition":{
        "StringLike":{
          "ses:FromDisplayName":"Marketing"
        }
      }
    }
  ]
}
```

Limitazione della destinazione del feedback su mancato recapito e reclamo

La policy seguente consente a un utente di chiamare le API di invio di e-mail SES, ma solo se "Return-Path" nell'e-mail è impostato su feedback@example.com.

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Action":[
        "ses:SendEmail",
        "ses:SendRawEmail"
      ],
      "Resource":"*",
      "Condition":{
        "StringEquals":{
          "ses:FeedbackAddress":"feedback@example.com"
        }
      }
    }
  ]
}
```

AWS politiche gestite per Amazon Simple Email Service

Per aggiungere autorizzazioni a utenti, gruppi e ruoli, è più facile utilizzare le politiche AWS gestite piuttosto che scriverle autonomamente. Creare policy gestite dal cliente IAM per fornire al tuo team solo le autorizzazioni di cui ha bisogno richiede tempo e competenza. Per iniziare rapidamente,

puoi utilizzare le nostre politiche AWS gestite. Queste politiche coprono casi d'uso comuni e sono disponibili nel tuo AWS account. Per ulteriori informazioni sulle policy AWS gestite, consulta le policy AWS gestite nella IAM User Guide.

AWS i servizi mantengono e aggiornano le politiche AWS gestite. Non è possibile modificare le autorizzazioni nelle politiche AWS gestite. I servizi aggiungono occasionalmente autorizzazioni aggiuntive a una policy AWS gestita per supportare nuove funzionalità. Questo tipo di aggiornamento interessa tutte le identità (utenti, gruppi e ruoli) a cui è collegata la policy. È più probabile che i servizi aggiornino una politica AWS gestita quando viene lanciata una nuova funzionalità o quando diventano disponibili nuove operazioni. I servizi non rimuovono le autorizzazioni da una policy AWS gestita, quindi gli aggiornamenti delle policy non comprometteranno le autorizzazioni esistenti.

Inoltre, AWS supporta politiche gestite per le funzioni lavorative che si estendono su più servizi. Ad esempio, la policy ReadOnlyAccess AWS gestita fornisce l'accesso in sola lettura a tutti i AWS servizi e le risorse. Quando un servizio lancia una nuova funzionalità, AWS aggiunge autorizzazioni di sola lettura per nuove operazioni e risorse. Per l'elenco e la descrizione delle policy di funzione dei processi, consulta la sezione Policy gestite da AWS per funzioni di processi nella Guida per l'utente di IAM.

AWS politica gestita: AmazonSES FullAccess

È possibile allegare la policy `AmazonSESFullAccess`alle identità IAM. Fornisce l'accesso completo ad Amazon SES.

Per visualizzare le autorizzazioni relative a questa politica, consulta AmazonSES FullAccess nel Managed Policy Reference.AWS

AWS politica gestita: AmazonSES ReadOnlyAccess

È possibile allegare la policy `AmazonSESReadOnlyAccess`alle identità IAM. Fornisce l'accesso di sola lettura ad Amazon SES.

Per visualizzare le autorizzazioni relative a questa politica, consulta AmazonSES ReadOnlyAccess nel Managed Policy Reference.AWS

AWS politica gestita: AmazonSES ServiceRolePolicy

Non è possibile allegare la policy `AmazonSESServiceRolePolicy` alle entità IAM. Questa policy è associata a un ruolo collegato al servizio che consente ad Amazon SES di eseguire azioni per tuo conto. Per ulteriori informazioni, consulta Autorizzazioni di ruolo collegate ai servizi per Amazon SES.

Per visualizzare le autorizzazioni relative a questa politica, consulta AmazonSES ServiceRolePolicy nel Managed Policy Reference.AWS

Amazon Simple Email Service: aggiornamenti alle politiche AWS gestite

Visualizza i dettagli e gli aggiornamenti delle politiche AWS gestite per Amazon Simple Email Service da quando questo servizio ha iniziato a tracciare queste modifiche.

Modifica	Descrizione	Data
Amazon Simple Email Service ha aggiunto una nuova policy gestita	Amazon Simple Email Service è stato aggiunto `AmazonSES ServiceRolePolicy` al ruolo collegato al servizio `AWSServiceRoleForA mazonSES` che consente a SES di eseguire azioni per tuo conto	13 maggio 2024
Amazon Simple Email Service ha aggiornato una definizione di policy	Amazon Simple Email Service ha chiarito che la voce precedente di questa tabella (riga sotto) era: Amazon Simple Email Service aggiunto `ses:BatchGetMetric Data` alla policy ReadOnlyA ccess gestita di AmazonSES , che consentirà l'accesso all'API SES BatchGetM etricData	30 aprile 2024
Amazon Simple Email Service ha aggiornato una definizione di policy	Amazon Simple Email Service è stato aggiunto `ses:Batch Get*` alla policy ReadOnlyA ccess gestita di AmazonSES: ciò consentirà l'accesso all'API SES BatchGetMetricData	16 febbraio 2024

Modifica	Descrizione	Data
Amazon Simple Email Service ha modificato due definizioni di policy	Amazon Simple Email Service rimosso «tramite la console di AWS gestione» dalla fine delle definizioni AmazonSES FullAccess e AmazonSES ReadOnlyAccess	3 maggio 2023
Amazon Simple Email Service ha iniziato a monitorare le modifiche	Amazon Simple Email Service ha iniziato a tracciare le modifiche alle sue politiche AWS gestite	5 aprile 2023

Utilizzo di ruoli collegati ai servizi per Amazon SES

Amazon Simple Email Service (SES) AWS Identity and Access Management utilizza ruoli collegati ai servizi (IAM). Un ruolo collegato ai servizi è un tipo unico di ruolo IAM collegato direttamente ad Amazon SES. I ruoli collegati ai servizi sono predefiniti da SES e includono tutte le autorizzazioni richieste dal servizio per chiamare altri servizi per tuo conto. AWS

Un ruolo collegato ai servizi semplifica la configurazione di SES perché non è necessario aggiungere manualmente le autorizzazioni necessarie. SES definisce le autorizzazioni dei suoi ruoli collegati ai servizi e, se non diversamente definito, solo SES può assumerne i ruoli. Le autorizzazioni definite includono la policy di attendibilità e la policy delle autorizzazioni che non può essere allegata a nessun'altra entità IAM.

È possibile eliminare un ruolo collegato ai servizi solo dopo aver eliminato le risorse correlate. Questo protegge le tue risorse SES perché non puoi rimuovere inavvertitamente l'autorizzazione ad accedere alle risorse.

Per informazioni sugli altri servizi che supportano i ruoli collegati al servizio, consulta Servizi AWS che funzionano con IAM e cerca i servizi che riportano Sì nella colonna Ruoli collegati al servizio. Scegli Sì in corrispondenza di un link per visualizzare la documentazione relativa al ruolo collegato al servizio per tale servizio.

Autorizzazioni di ruolo collegate ai servizi per Amazon SES

SES utilizza il ruolo collegato al servizio denominato AWSServiceRoleForAmazonSES: consente a SES di pubblicare i parametri CloudWatch di monitoraggio di base di Amazon per conto delle tue risorse SES.

Il ruolo AWSServiceRoleForAmazonSES collegato al servizio si affida al seguente servizio per l'assunzione del ruolo:

- `ses.amazonaws.com`

La politica di autorizzazione dei ruoli denominata AmazonSES ServiceRolePolicy è una politica AWS gestita che consente a SES di completare le seguenti azioni sulle risorse specificate:

- Azione: `cloudwatch:PutMetricData` nello spazio dei nomi. `AWS/SES` CloudWatch Questa azione concede il permesso a SES di inserire dati metrici nel namespace. CloudWatch `AWS/SES` Per ulteriori informazioni sulle metriche SES disponibili in, consulta. CloudWatch Registrazione e monitoraggio in Amazon SES
- Azione: `cloudwatch:PutMetricData` nello `AWS/SES/MailManager` CloudWatch spazio dei nomi. Questa azione concede il permesso a SES di inserire dati metrici nel namespace. CloudWatch `AWS/SES/MailManager` Per ulteriori informazioni sulle metriche SES disponibili in, consulta. CloudWatch Registrazione e monitoraggio in Amazon SES
- Azione: `cloudwatch:PutMetricData` nello `AWS/SES/Addons` CloudWatch spazio dei nomi. Questa azione concede il permesso a SES di inserire dati metrici nel namespace. CloudWatch `AWS/SES/Addons` Per ulteriori informazioni sulle metriche SES disponibili in, consulta. CloudWatch Registrazione e monitoraggio in Amazon SES

Per consentire a utenti, gruppi o ruoli di creare, modificare o eliminare un ruolo orientato ai servizi, devi configurare le autorizzazioni. Per ulteriori informazioni, consulta Autorizzazioni del ruolo collegato ai servizi nella Guida per l'utente di IAM.

Creazione di un ruolo collegato ai servizi per Amazon SES

Non hai bisogno di creare manualmente un ruolo collegato ai servizi. Quando crei risorse SES nella AWS Management Console, o nell' AWS API AWS CLI, SES crea automaticamente il ruolo collegato al servizio.

Se elimini questo ruolo collegato ai servizi, puoi ricrearlo seguendo lo stesso processo utilizzato per ricreare il ruolo nell'account. Quando crei risorse SES, SES crea nuovamente il ruolo collegato ai servizi per te.

Modifica di un ruolo collegato al servizio per Amazon SES

SES non consente di modificare il ruolo collegato al AWSServiceRoleForAmazonSES servizio. Dopo aver creato un ruolo collegato al servizio, non potrai modificarne il nome perché varie entità potrebbero farvi riferimento. È possibile tuttavia modificarne la descrizione utilizzando IAM.

Eliminazione di un ruolo collegato al servizio per SES

Se non è più necessario utilizzare una funzionalità o un servizio che richiede un ruolo collegato al servizio, ti consigliamo di eliminare il ruolo. In questo modo non sarà più presente un'entità non utilizzata che non viene monitorata e gestita attivamente. Tuttavia, è necessario effettuare la pulizia delle risorse associate al ruolo collegato ai servizi prima di poterlo eliminare manualmente.

Pulizia di un ruolo collegato al servizio

Prima di poter utilizzare IAM per eliminare un ruolo collegato al servizio, è necessario eliminare tutte le risorse SES.

> **Note**
>
> Se il servizio SES utilizza il ruolo quando si tenta di eliminare le risorse, l'eliminazione potrebbe non riuscire. In questo caso, attendi alcuni minuti e quindi ripeti l'operazione.

Eliminazione manuale del ruolo collegato ai servizi

Utilizza la console IAM AWS CLI, o l' AWS API per eliminare il ruolo AWSServiceRoleForAmazonSES collegato al servizio. Per ulteriori informazioni, consulta Eliminazione del ruolo collegato al servizio nella Guida per l'utente di IAM.

Regioni supportate per i ruoli collegati ai servizi Amazon SES

SES non supporta l'utilizzo di ruoli collegati al servizio in tutte le regioni in cui il servizio è disponibile. È possibile utilizzare il AWSServiceRoleForAmazonSES ruolo nelle seguenti regioni.

Nome Regione	Identità della regione	Support in SES
US East (N. Virginia)	us-east-1	Sì
Stati Uniti orientali (Ohio)	us-east-2	Sì
Asia Pacifico (Sydney)	ap-southeast-2	Sì
Asia Pacifico (Tokyo)	ap-northeast-1	Sì
Europe (Frankfurt)	eu-central-1	Sì
Europa (Irlanda)	eu-west-1	Sì

Registrazione e monitoraggio in Amazon SES

Il monitoraggio è importante per mantenere l'affidabilità, la sicurezza, la disponibilità e le prestazioni di Amazon SES e delle soluzioni AWS. AWS offre vari strumenti che aiutano a monitorare Amazon SES e rispondere a potenziali incidenti.

- Amazon CloudWatch monitora le risorse AWS e le applicazioni che esegui su AWS in tempo reale. Puoi raccogliere i parametri e tenerne traccia, creare pannelli di controllo personalizzati e impostare allarmi per inviare una notifica o intraprendere azioni quando un parametro specificato raggiunge una determinata soglia. Per ulteriori informazioni, consulta Recupero di dati relativi a eventi di Amazon SES da CloudWatch e Creazione di allarmi di monitoraggio della reputazione tramite CloudWatch.
- AWS CloudTrail acquisisce le chiamate API e gli eventi correlati effettuati da o per conto del tuo Account AWS e fornisce i file di log a un bucket Amazon S3 specificato. Puoi identificare quali utenti e account hanno richiamato AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute. Per ulteriori informazioni, consulta Registrazione delle chiamate API di Amazon SES con AWS CloudTrail.
- Gli eventi di invio di e-mail Amazon SES possono aiutarti a perfezionare la tua strategia di invio e-mail. Amazon SES acquisisce informazioni dettagliate, inclusi i numeri di invii, consegne, aperture, clic, mancate recapiti, reclami e rifiuti. Per ulteriori informazioni, consulta Monitoraggio dell'attività di invio.
- I parametri di reputazione Amazon SES rilevano le percentuali di mancati recapiti e reclami. Per ulteriori informazioni, consulta Monitoraggio della reputazione del mittente.

Registrazione delle chiamate API di Amazon SES con AWS CloudTrail

Amazon SES è integrato con AWS CloudTrail, un servizio che offre un record delle operazioni eseguite da un utente, un ruolo o un servizio AWS in Amazon SES. CloudTrail acquisisce le chiamate API per Amazon SES come eventi. Le chiamate acquisite includono le chiamate dalla console Amazon SES e le chiamate di codice alle operazioni API di Amazon SES. Se crei un percorso, puoi abilitare la distribuzione continua di eventi CloudTrail in un bucket Amazon S3, inclusi gli eventi per Amazon SES. Se non configuri un percorso, è comunque possibile visualizzare gli eventi più recenti nella console di CloudTrail in Event history (Cronologia eventi). Le informazioni raccolte da CloudTrail consentono di determinare la richiesta effettuata ad Amazon SES, l'indirizzo IP da cui è partita la richiesta, l'autore della richiesta, il momento in cui è stata eseguita e altri dettagli.

Per ulteriori informazioni su CloudTrail, incluso come configurarlo e abilitarlo, consulta la AWS CloudTrail Guida per l'utente.

Informazioni su Amazon SES in CloudTrail

CloudTrail è abilitato sul tuo Account AWS al momento della sua creazione. Quando si verifica un'attività supportata in Amazon SES, questa viene registrata in un evento CloudTrail insieme ad altri eventi del servizio AWS in Event history (Cronologia eventi). Puoi visualizzare, cercare e scaricare gli eventi recenti nell'Account AWS. Per ulteriori informazioni, consulta Visualizzazione di eventi mediante la cronologia eventi di CloudTrail.

Per una registrazione continua degli eventi nel tuo Account AWS, inclusi gli eventi per Amazon SES, crea un percorso. Un percorso consente a CloudTrail di distribuire i file di log in un bucket Amazon S3. Per impostazione predefinita, quando si crea un percorso nella console, questo sarà valido in tutte le Regioni AWS. Il percorso registra gli eventi di tutte le Regioni nella partizione AWS e distribuisce i file di log nel bucket Amazon S3 specificato. Inoltre, è possibile configurare altri servizi AWS per analizzare con maggiore dettaglio e usare i dati evento raccolti nei log CloudTrail. Per ulteriori informazioni, consulta gli argomenti seguenti:

- Panoramica della creazione di un percorso
- Servizi e integrazioni CloudTrail supportati
- Configurazione delle notifiche Amazon SNS per CloudTrail
- Ricezione di file di log CloudTrail da più regioni e Ricezione di file di log CloudTrail da più account

Amazon SES supporta la registrazione di tutte le azioni elencate nella documentazione di riferimento all'API SES e nella documentazione di riferimento all'API SES v2 come eventi nei file di log CloudTrail, ad eccezione di quelle elencate nella seguente nota.

> **Note**
>
> Amazon SES invia eventi di gestione a CloudTrail. Gli eventi di gestione includono operazioni correlate alla creazione e alla gestione delle risorse all'interno del tuo Account AWS. In Amazon SES, gli eventi di gestione includono operazioni quali la creazione e l'eliminazione di identità o regole di ricezione.
> Gli eventi di gestione differiscono dagli eventi dei dati. Gli eventi dei dati sono eventi correlati all'accesso e all'interazione con i dati all'interno del tuo Account AWS. In Amazon SES, gli eventi dei dati includono operazioni come l'invio di e-mail.
> Poiché Amazon SES distribuisce solo gli eventi di gestione a CloudTrail, i seguenti eventi non vengono registrati in CloudTrail:
>
> - SendEmail
> - SendRawEmail
> - SendTemplatedEmail
> - SendBulkTemplatedEmail
>
> Puoi utilizzare la pubblicazione di eventi per registrare gli eventi correlati all'invio di e-mail. Per ulteriori informazioni, consulta Monitoraggio dell'invio di e-mail utilizzando la pubblicazione di eventi di Amazon SES.

Ogni evento o voce di registro contiene informazioni sull'utente che ha generato la richiesta. Le informazioni di identità consentono di determinare quanto segue:

- Se la richiesta è stata effettuata con credenziali utente root o AWS Identity and Access Management (IAM).
- Se la richiesta è stata effettuata con le credenziali di sicurezza temporanee per un ruolo o un utente federato.
- Se la richiesta è stata effettuata da un altro servizio AWS.

Per ulteriori informazioni, consulta Elemento userIdentity di CloudTrail.

Esempio: voci del file di log di Amazon SES

Un percorso è una configurazione che consente la distribuzione di eventi come i file di log in un bucket Amazon S3 da te specificato. I file di log di CloudTrail possono contenere una o più voci di log. Un evento rappresenta una singola richiesta da un'origine e include informazioni sull'operazione richiesta, sulla data e sull'ora dell'operazione, sui parametri richiesti e così via. I file di log CloudTrail non sono una traccia di stack ordinata delle chiamate API pubbliche e, di conseguenza, non devono apparire in base a un ordine specifico.

L'esempio seguente mostra una voce di registro di CloudTrail che illustra l'operazione `DeleteIdentity` o `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"
      }
    }
  ]
}
```


Convalida della conformità per Amazon Simple Email Service

Revisori di terze parti valutano la sicurezza e la conformità di Amazon Simple Email Service come parte di più programmi di conformità di AWS. Questi includono SOC, PCI, FedRAMP, HIPAA e altri.

Per un elenco dei servizi AWS che rientrano nell'ambito di programmi di conformità specifici, consulta Servizi AWS che rientrano nell'ambito del programma di conformità . Per informazioni generali, consulta Programmi per la conformità di AWS.

È possibile scaricare i report di audit di terze parti utilizzando AWS Artifact. Per ulteriori informazioni, consulta Download di report in AWS Artifact.

La responsabilità per la conformità quando utilizzi Amazon Simple Email Service è determinata dalla riservatezza dei dati, dagli obiettivi di conformità dell'azienda e dalle normative vigenti. AWS fornisce le risorse seguenti per semplificare la conformità:

- Guide rapide per la sicurezza e la conformità: queste guide alla distribuzione illustrano considerazioni relative all'architettura e forniscono i passaggi per la distribuzione di ambienti di base incentrati sulla sicurezza e sulla conformità su AWS.

- Whitepaper sulla progettazione per la sicurezza HIPAA e la conformità: questo whitepaper descrive in che modo le aziende possono utilizzare AWS per creare applicazioni conformi ai requisiti HIPAA.
- Risorse per la conformità AWS: una raccolta di cartelle di lavoro e guide suddivise per settore e area geografica.
- Valutazione delle risorse con le regole nella Guida per gli sviluppatori di AWS Config: AWS Config valuta il livello di conformità delle configurazioni delle risorse con pratiche interne, linee guida e regolamenti industriali.
- AWS Security Hub: Questo servizio AWS fornisce una visione completa dello stato di sicurezza all'interno di AWS che consente di verificare la conformità con gli standard e le best practice di sicurezza del settore.

Resilienza in Amazon Simple Email Service

L'infrastruttura globale di AWS è basata su regioni AWS e zone di disponibilità. Le regioni forniscono più zone di disponibilità fisicamente separate e isolate, connesse tramite reti altamente ridondanti, a bassa latenza e throughput elevato. Con le zone di disponibilità, è possibile progettare e gestire applicazioni e database che eseguono il failover automatico tra zone di disponibilità senza interruzioni. Le zone di disponibilità sono più disponibili, tolleranti ai guasti e scalabili rispetto alle infrastrutture a data center singolo o multiplo.

Per ulteriori informazioni sulle regioni AWS e sulle zone di disponibilit, consulta Infrastruttura globale di AWS.

Sicurezza dell'infrastruttura in Amazon Simple Email Service

In qualità di servizio gestito, Amazon Simple Email Service è protetto dalla sicurezza della rete globale AWS. Per informazioni sui servizi di sicurezza AWS e su come AWS protegge l'infrastruttura, consulta la pagina Sicurezza del cloud AWS. Per progettare l'ambiente AWS utilizzando le best practice per la sicurezza dell'infrastruttura, consulta la pagina Protezione dell'infrastruttura nel Pilastro della sicurezza di AWS Well-Architected Framework.

Utilizza le chiamate API pubblicate di AWS per accedere ad Amazon Simple Email Service tramite la rete. I clienti devono supportare quanto segue:

- Transport Layer Security (TLS). È richiesto TLS 1.2 ed è consigliato TLS 1.3.

- Suite di cifratura con Perfect Forward Secrecy (PFS), ad esempio Ephemeral Diffie-Hellman (DHE) o Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). La maggior parte dei sistemi moderni, come Java 7 e versioni successive, supporta tali modalità.

Inoltre, le richieste devono essere firmate utilizzando un ID chiave di accesso e una chiave di accesso segreta associata a un principale IAM. In alternativa, è possibile utilizzare AWS Security Token Service (AWS STS) per generare le credenziali di sicurezza temporanee per sottoscrivere le richieste.

Configurazione degli endpoint VPC per Amazon SES

Molti clienti Amazon SES hanno policy aziendali che limitano la capacità dei loro sistemi interni di connettersi a Internet pubblico. Queste policy impediscono l'utilizzo degli endpoint pubblici Amazon SES.

Se disponi di policy simili, puoi lavorare all'interno di queste restrizioni utilizzando Amazon Virtual Private Cloud. Con Amazon VPC, puoi distribuire AWS risorse in una rete virtuale che esiste in un'area isolata del. Cloud AWS Per ulteriori informazioni su Amazon VPC, consulta la Guida per l'utente di Amazon VPC.

Puoi connetterti direttamente da Amazon VPC a SES tramite un endpoint VPC in modo sicuro e scalabile. L'utilizzo di un endpoint VPC dell'interfaccia offre un migliore assetto di sicurezza in quanto non è necessario aprire firewall per il traffico in uscita, nonché altri vantaggi derivanti dall'utilizzo degli endpoint Amazon VPC.

Quando si utilizza un endpoint VPC, il traffico verso SES non viene trasmesso su Internet e non lascia mai la rete Amazon per stabilire una connessione sicura del VPC a SES senza rischi di disponibilità o vincoli di larghezza di banda sul traffico di rete. Puoi centralizzare SES nella tua infrastruttura multi-account e fornirlo come un servizio ai tuoi account senza dover utilizzare un gateway Internet.

Limitazioni

- SES non supporta endpoint VPC nelle seguenti zone di disponibilità: `use1-az2`, `use1-az3`, `use1-az5`, `usw1-az2`, `usw2-az4`, `apne2-az4`, `cac1-az3` e `cac1-az4`.
- L'endpoint SMTP utilizzato nel VPC è limitato alla Regione AWS attualmente utilizzata per il proprio account.

Esempio di procedura dettagliata di configurazione di SES in Amazon VPC

Prerequisiti

Prima di eseguire la procedura descritta in questa sezione, è necessario completare i seguenti passaggi:

- Disporre di un cloud privato virtuale (VPC) o creare un nuovo VPC. Per le procedure, consultare Nozioni di base su Amazon VPC.
- Avviare un'istanza di Amazon EC2 nel VPC per eseguire il test della connettività all'endpoint VPC creato in un passaggio successivo. Per ulteriori informazioni, consultare VPC di default.

> **Note**
>
> Sebbene sia possibile utilizzare gli endpoint VPC per SES con qualsiasi risorsa, per semplificare il metodo di test, in questo esempio verrà richiesto di utilizzare un'istanza EC2 come risorsa. Poiché Amazon EC2 limita il traffico e-mail sulla porta 25 per impostazione predefinita, sarà necessario utilizzare una porta diversa da TCP 25, ad esempio TCP 465, 587, 2465 o 2587.

Configurazione di SES in Amazon VPC

Il processo di configurazione di un endpoint VPC da utilizzare con SES è costituito da alcuni passaggi separati. Innanzitutto, è necessario creare un gruppo di sicurezza che consenta all'istanza di comunicare con le porte SMTP, quindi creare un endpoint VPC per Amazon SES e infine eseguire il test della connessione all'endpoint VPC per assicurarsi che sia configurato correttamente.

Fase 1: creazione del gruppo di sicurezza

In questa fase viene creato un gruppo di sicurezza che consente alle istanze Amazon EC2 di comunicare con l'endpoint dell'interfaccia VPC che si sta creando.

Creazione del gruppo di sicurezza

1. Nel pannello di navigazione della console Amazon EC2, in Network & Security (Rete e sicurezza), selezionare Security Groups (Gruppi di sicurezza).
2. Scegliere Create Security Group (Crea gruppo di sicurezza).
3. In Basic details (Dettagli di base), eseguire le operazioni seguenti:

- In Security group name (Nome gruppo di sicurezza), immettere un nome univoco che identifichi il gruppo di sicurezza.
- Per Description (Descrizione), è possibile immettere un testo che descriva lo scopo del gruppo di sicurezza.
- Per VPC, scegliere il VPC che si desidera far utilizzare ad Amazon SES.

4. Per Inbound rules (Regole in entrata), scegliere Add rule (Aggiungi regola).
5. Per la nuova Regola in entrata, effettuare le seguenti operazioni:

   - Per Type (Tipo), scegliere Custom TCP (TCP personalizzato).
   - Per Port range (Intervallo porte), immettere il numero di porta che si desidera utilizzare per inviare e-mail. È possibile utilizzare uno dei seguenti numeri di porta: **465**, **587**, **2465**, o **2587**.
   - Per Source type (Tipo di origine), scegliere Custom (Personalizzato).
   - Per Origine, inserire l'intervallo IP CIDR o altri ID del gruppo di sicurezza contenenti le risorse che verranno utilizzate dall'endpoint VPC per comunicare con il servizio SES.
   - Ripetere i passaggi 4 e 5 per ogni intervallo CIDR o gruppo di sicurezza da cui si desidera consentire l'accesso.

6. Al termine, scegliere Create security group (Crea gruppo di sicurezza).

Fase 2: creazione dell'endpoint VPC

In Amazon VPC, un endpoint VPC ti consente di connettere il tuo VPC ai servizi supportati. AWS In questo caso, Amazon VPC viene configurato in modo che il gruppo di sicurezza Amazon EC2 possa connettersi ad Amazon SES.

Creazione dell'endpoint VPC

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. In Virtual Private Cloud (Cloud virtuale privato), scegliere Endpoints (Endpoint).
3. Scegli Create Endpoint (Crea endpoint) per aprire la pagina Create Endpoint (Crea endpoint).
4. (Facoltativo) Nel pannello Endpoint settings (Impostazioni endpoint), crea un tag nel campo Name tag (Tag nome).
5. In Categoria del servizio, seleziona Servizi AWS .
6. Nel pannello Services (Servizi), filtra per smtp nella barra di ricerca, quindi seleziona il relativo pulsante di opzione.

7. Nel pannello VPC, fai clic all'interno della barra di ricerca e seleziona un VPC dalla casella dell'elenco (consulta the section called “Prerequisiti”).
8. Nel pannello Subnets (Sottoreti), seleziona Availability Zones (Zone di disponibilità) e Subnet IDs (ID di sottorete).

   > **Note**
   >
   > Amazon SES non supporta endpoint VPC nelle seguenti Zone di disponibilità: `use1-az2`, `use1-az3`, `use1-az5`, `usw1-az2`, `usw2-az4`, `apne2-az4`, `cac1-az3` e `cac1-az4`.

9. Nel pannello Security groups (Gruppi di sicurezza), seleziona il gruppo di sicurezza creato in precedenza.
10. (Facoltativo) Puoi creare uno o più tag nel pannello Tag.
11. Selezionare Create endpoint (Crea endpoint). Attendere circa 5 minuti mentre Amazon VPC crea l'endpoint. Quando l'endpoint è pronto per l'uso, il valore nella colonna Status (Stato) diventa Available (Disponibile).

(Facoltativo) Fase 3: test della connessione all'endpoint VPC

Al termine del processo di configurazione dell'endpoint VPC, puoi eseguire il test della connessione per assicurarti che l'endpoint VPC sia configurato correttamente. È possibile testare la connessione utilizzando gli strumenti a riga di comando inclusi nella maggior parte dei sistemi operativi.

Verifica della connessione all'endpoint VPC

1. Avvia un'istanza Amazon EC2 nello stesso VPC in cui hai creato l’endpoint VPC email-smtp.

   Per informazioni sulla connessione alle istanze Linux, consulta Connect to your Linux istance nella Amazon EC2 User Guide.

   Per informazioni sulla connessione alle istanze Windows, consulta il tutorial introduttivo nella Guida per l'utente di Amazon EC2.
2. Invia un'e-mail di prova, ad esempio, utilizzando l'interfaccia SMTP SES.

> **Note**
>
> È necessario verificare un indirizzo e-mail o un dominio prima di poter inviare e-mail tramite Amazon SES. Per ulteriori informazioni sulla verifica delle identità, consulta Creazione e verifica delle identità in Amazon SES.

Risoluzione dei problemi di Amazon SES

In questa sezione sono inclusi i seguenti argomenti che possono risultare utili quando si verificano problemi:

- Per informazioni sui problemi di verifica del dominio potenziali che potresti incontrare, consulta Problemi di verifica del dominio e dell'indirizzo e-mail.
- Per le soluzioni ai problemi relativi a DKIM, consulta Risoluzione dei problemi relativi a DKIM in Amazon SES.
- Per un elenco dei problemi di recapito comuni che potresti incontrare durante l'invio di e-mail, con le operazioni che si possono eseguire per correggerli, consulta Problemi di recapito di Amazon SES.
- Per una descrizione dei problemi che i destinatari possono incontrare quando ricevono un'e-mail che è stata inviata tramite Amazon SES, consulta Problemi con le e-mail ricevute da Amazon SES.
- Per soluzioni a problemi di notifica di recapito, mancato recapito e reclamo, consulta Problemi di notifica di Amazon SES.
- Per un elenco degli errori che possono verificarsi quando si invia un'e-mail con Amazon SES, consulta Errori di invio di e-mail con Amazon SES.
- Per suggerimenti su come aumentare la velocità di invio delle e-mail quando effettui chiamate multiple ad Amazon SES utilizzando l'API o l'interfaccia SMTP, consulta Aumento della velocità effettiva con Amazon SES.
- Per le soluzioni ai problemi comuni che possono verificarsi quando utilizzi Amazon SES tramite l'interfaccia SMTP (Simple Mail Transfer Protocol), nonché l'elenco dei codici di risposta SMTP restituiti da Amazon SES, consulta Problemi relativi a SMTP in Amazon SES.
- Per un elenco dei codici di errore comuni che vengono restituiti dall'API Amazon SES v2, consulta Errori comuni.
- Per una descrizione dei problemi più comuni correlati al nostro processo di verifica di invio e su come gestirli, consulta Domande frequenti sul processo di verifica dell'invio di Amazon SES.
- Per una discussione su come le liste blackhole basate su DNS (DNSBL) influiscono sull'invio con Amazon SES, consulta Domande frequenti sulla DNS Blackhole List (DNSBL).

Se chiami l'API Amazon SES direttamente, consulta il Documento di riferimento per l'API Amazon Simple Email Service per gli errori HTTP che potresti ricevere.

> **Note**
>
> Se hai bisogno di assistenza, non utilizzare il link per l'invio di feedback in questa pagina, perché il modulo viene ricevuto dal team della documentazione AWS e non dal team di supporto AWS. Per esplorare le diverse opzioni di supporto disponibili, vai alla pagina Contattaci.

Indice

Problemi generali di Amazon SES

Le informazioni contenute in questa pagina illustrano e aiutano a diagnosticare i problemi che possono verificarsi quando si utilizza Amazon SES.

Le modifiche che apporto non sono immediatamente visibili

Poiché si tratta di un servizio a cui si accede da computer in data center presenti in tutto il mondo, Amazon SES utilizza un modello di elaborazione distribuito denominato consistenza finale. È necessario del tempo affinché le modifiche apportate in Amazon SES (o in altri servizi AWS) risultino visibili da tutti i possibili endpoint. Alcuni dei ritardi sono dovuti al tempo necessario per inviare i dati da un server a un altro e da una regione a un'altra nel mondo. Nella maggior parte dei casi, questo ritardo non sarà superiore a pochi minuti.

Tra le aree in cui può verificarsi un ritardo sono incluse:

- Creazione e modifica di set di configurazione: quando si crea o si modifica un set di configurazione (ad esempio, se si associa un pool di indirizzi IP dedicati a un set di configurazione esistente), vi potrebbe essere un breve ritardo dal momento in cui viene creato o modificato al momento in cui le modifiche sono attive.
- Creazione e modifica di destinazioni di eventi: quando si crea o si modifica una destinazione di evento (ad esempio, si comunica ad Amazon SES di inviare i dati relativi all'invio di e-mail a un altro servizio AWS), vi potrebbe essere un ritardo dal momento in cui la destinazione di evento viene creata o modificata al momento in cui gli eventi di invio e-mail raggiungono effettivamente la destinazione specificata.

Problemi di verifica del dominio e dell'indirizzo e-mail

La procedura di verifica di un indirizzo e-mail o un dominio con Amazon SES, viene avviata utilizzando la console o l'API di Amazon SES. In questa sezione sono incluse informazioni che possono aiutare a risolvere problemi con la procedura di verifica.

> **Note**
>
> Nelle procedure seguenti, il riferimento ai registri DNS potrebbe riferirsi al registro CNAME o TXT a seconda della forma di DKIM utilizzata. Easy DKIM utilizza i registri CNAME e Bring Your Own DKIM (BYODKIM) utilizza i registri TXT. Sono previste procedure di verifica dettagliate per ciascuna delle Easy DKIM o BYODKIM.

Problemi comuni di verifica dei domini

Di seguito sono elencate le possibili cause e soluzioni per eventuali problemi riscontrati durante la verifica di un dominio mediante la procedura descritta in the section called “Verifica di un'identità dominio”.

- Stai cercando di verificare un dominio che non ti appartiene: non puoi verificare un dominio che non ti appartiene. Se ad esempio desideri inviare e-mail tramite Amazon SES da un indirizzo sul dominio gmail.com, devi verificare questo indirizzo e-mail in modo specifico. Non puoi verificare l'intero dominio gmail.com.
- Stai tentando di verificare un dominio privato: non puoi verificare un dominio se i registri DNS TXT non possono essere risolti tramite DNS pubblico.

- Il tuo provider di DNS non consente l'utilizzo di trattini di sottolineatura nei nomi dei registri TXT: alcuni provider di DNS non consentono di includere il carattere di sottolineatura nel record DNS per i tuoi nomi di registro. Tuttavia, la sottolineatura nel nome di record DKIM è obbligatoria. Se il provider di DNS non consente di inserire un segno di sottolineatura nel nome del record, contatta il team di assistenza clienti del provider per ricevere assistenza.
- Il tuo provider di DNS ha accodato il nome di dominio alla fine del registro DNS: alcuni provider di DNS accodano automaticamente il nome di dominio al nome di attributo del registro DNS. Ad esempio, se crei un record in cui il nome di attributo è _domainkey.example.com, il provider potrebbe aggiungere il nome di dominio, generando _domainkey.example.com.example.com). Per evitare tale duplicazione del nome di dominio, aggiungi un punto alla fine del nome di dominio nel record DNS. Questo fase indica al tuo provider di DNS che non è necessario accodare il nome di dominio per il registro.
- Il provider DNS ha modificato il valore del record DNS.: alcuni provider modificano automaticamente i valori dei record DNS per utilizzare solo lettere minuscole. Il dominio viene verificato solo quando Amazon SES rileva un record di verifica per il quale il valore dell'attributo corrisponde esattamente al valore fornito all'avvio del processo di verifica della proprietà del dominio. Se il provider di DNS per il dominio cambia i valori del registro DNS affinché siano utilizzate solo lettere minuscole, contatta il provider di DNS per ulteriore assistenza.
- Vuoi verificare lo stesso dominio più volte: potresti dover verificare il tuo dominio più di una volta in quanto stai effettuando l'invio in regioni diverse oppure perché stai utilizzando lo stesso dominio per inviare messaggi da più account AWS. Se il provider di DNS non consente di disporre di più di un record TXT con lo stesso nome di attributo, potresti comunque essere in grado di verificare due domini. Se il provider DNS lo consente, puoi assegnare più valori di attributo al medesimo record DNS. Ad esempio, se il tuo DNS viene gestito da Amazon Route 53, puoi impostare più valori per lo stesso registro CNAME completando le seguenti fasi:

  1. Nella console Route 53, seleziona il registro CNAME creato al momento della verifica del dominio nella prima regione.
  2. Nella casella Value (Valore), vai alla fine del valore di attributo esistente e quindi premi Invio.
  3. Aggiungi il valore di attributo per la regione aggiuntiva e salva il set di record.

  Se il provider di DNS non consente di assegnare più valori per lo stesso registro DNS, puoi verificare il dominio una volta con _domainkey nel nome di attributo del registro DNS e un'altra volta con _domainkey rimosso dal nome di attributo. Lo svantaggio di questa soluzione è puoi verificare lo stesso dominio soltanto due volte.

Controllo delle impostazioni di verifica del dominio

Puoi controllare che il registro DNS di verifica del dominio Amazon SES sia stato pubblicato correttamente nel server DNS utilizzando la procedura seguente. Questa procedura si avvale dello strumento nslookup, disponibile per Windows e Linux. In Linux è possibile usare anche dig.

I comandi di queste istruzioni sono stati eseguiti in Windows 7 e il dominio di esempio che utilizziamo è ses-example.com configurato con Easy DKIM che usa registri CNAME.

In questa procedura occorre prima individuare i server DNS del tuo dominio, quindi eseguire query su tali server per visualizzare i registri CNAME. Si eseguono query sui server DNS del tuo dominio perché questi server contengono le informazioni più aggiornate sul dominio, la cui propagazione ad altri server DNS può richiedere tempo.

Per verificare che i registri CNAME di verifica del dominio siano stati pubblicati nel server DNS

1. Trova i server di nomi per il tuo dominio con la procedura seguente.

   a. Accedi alla riga di comando. Per visualizzare la riga di comando in Windows 7, scegli Start (Avvia) e digita cmd. Nei sistemi operativi basati su Linux apri una finestra di terminale.

   b. Al prompt dei comandi digita il comando seguente, dove **<domain>** è il tuo dominio. Verranno elencati tutti i server utilizzati dal tuo dominio.

      ```
      nslookup -type=NS <domain>
      ```

      Se il dominio fosse ses-example.com, questo comando avrebbe il seguente aspetto:

      ```
      nslookup -type=NS ses-example.com
      ```

      L'output del comando elenca i server dei nomi utilizzati dal tuo dominio. Eseguirai query su uno di questi server di nella fase successiva.

2. Verifica che i registri CNAME siano pubblicati correttamente con la procedura seguente. Tieni presente che Amazon SES genera tre registri CNAME per l'autenticazione Easy DKIM, quindi ripeti le seguenti procedure per ciascuno dei tre.

   a. Al prompt dei comandi digita il comando seguente, dove **<random string>** è il nome CNAME generato da SES, **<domain>** è il tuo dominio e **<name server>** è uno dei server dei nomi trovati nella fase 1.

```
nslookup -type=CNAME <random string>_domainkey.<domain> <name server>
```

Nel nostro esempio ses-example.com, se un server dei nomi trovato nella fase 1 fosse denominato ns1.name-server.net e **<**random string**>** generata da SES è `4hzwn5lmznmmjyl2pqf2agr3uzzzzxyz`, digiteremmo:

```
nslookup -type=CNAME 4hzwn5lmznmmjyl2pqf2agr3uzzzzxyz_domainkey.ses-example.com
 ns1.name-server.net
```

b. Nell'output del comando verifica che la stringa che segue `canonical name =` corrisponda al valore CNAME che visualizzi quando scegli il dominio nell'elenco delle identità della console Amazon SES.

   Nel nostro esempio cerchiamo un registro CNAME in `4hzwn5lmznmmjyl2pqf2agr3uzzzzxyz_domainkey.ses-example.com` con il valore `4hzwn5lmznmmjyl2pqf2agr3uzzzzxyz.dkim.amazonses.com`. Se il record viene pubblicato correttamente, il comando dovrebbe avere l'output seguente:

```
4hzwn5lmznmmjyl2pqf2agr3uzzzzxyz_domainkey.ses-example.com canonical name =
 "4hzwn5lmznmmjyl2pqf2agr3uzzzzxyz.dkim.amazonses.com"
```

Problemi comuni di verifica degli indirizzi e-mail

- L'e-mail di verifica non è arrivata: se hai completato le procedure indicate in Verifica di un'identità indirizzo e-mail ma non hai ricevuto l'e-mail di verifica entro pochi minuti, completa i seguenti passaggi:
  - Controlla la cartella dello spam e della posta indesiderata per l'indirizzo e-mail che stai tentando di verificare.
  - Verifica che l'indirizzo che stai provando a verificare sia in grado di ricevere e-mail. Utilizzando un indirizzo e-mail separato (ad esempio il tuo indirizzo e-mail personale), invia un messaggio e-mail di prova all'indirizzo che desideri verificare.
  - Controlla l'elenco degli indirizzi verificati nella console Amazon SES. Assicurati che non vi siano errori nell'indirizzo e-mail che stai tentando di verificare.

Risoluzione dei problemi relativi a DKIM in Amazon SES

In questa sezione sono elencati alcuni dei problemi che possono verificarsi quando si configura l'autenticazione DKIM in Amazon SES. Se si tenta di configurare DKIM e si verificano problemi, esaminare le possibili cause e soluzioni riportate di seguito.

Hai configurato DKIM con successo, ma i messaggi non vengono firmati con DKIM

Se è stato utilizzato Easy DKIM o BYODKIM per configurare DKIM per un dominio, ma i messaggi inviati non sono provvisti di firma DKIM, effettuare le seguenti operazioni:

- Assicurati che DKIM sia abilitato per l'identità appropriata. Per abilitare DKIM per un'identità nella console Amazon SES, scegli il dominio e-mail nell'elenco Identities (Identità). Nella pagina dei dettagli del dominio espandi DKIM, quindi scegli Enable (Abilita) per abilitare DKIM.
- Assicurati di non inviare da un indirizzo e-mail verificato sullo stesso dominio. Se si imposta DKIM per un dominio, tutti i messaggi inviati da tale dominio sono firmati da DKIM, ad eccezione degli indirizzi di posta elettronica verificati singolarmente. Gli indirizzi e-mail verificati singolarmente usano impostazioni separate. Ad esempio, se hai configurato DKIM per il dominio example.com e hai verificato separatamente l'indirizzo e-mail mary@example.com (ma non hai configurato DKIM per l'indirizzo), i messaggi e-mail inviati da mary@example.com vengono inviati senza autenticazione DKIM. È possibile risolvere questo problema eliminando l'identità dell'indirizzo di posta elettronica dall'elenco di identità per l'account.
- Se si utilizza la stessa identità in più di una regione AWS, è necessario configurare DKIM per ciascuna regione separatamente. Allo stesso modo, se si utilizza lo stesso dominio con più di un account AWS, è necessario configurare DKIM per ogni account. Se si rimuovono i record DNS necessari per una Regione o un account specifici, Amazon SES disabilita la firma DKIM in tale Regione o account. Se la firma DKIM viene disabilitata, Amazon SES invia una notifica via e-mail.

I dettagli DKIM del tuo dominio nella console Amazon SES mostrano il messaggio DKIM: waiting on sender verification...(DKIM: in attesa di verifica del mittente in...) Stato di verifica DKIM: in attesa di verifica.

Se si completano le procedure in Easy DKIM o BYODKIM (Bring Your Own DKIM) per configurare DKIM per un dominio, ma la console Amazon SES indica ancora che la verifica DKIM è in sospeso, eseguire le operazioni seguenti:

- Attendere fino a 72 ore. In rari casi, rendere visibili i record DNS ad Amazon SES può richiedere tempo.

- Verificare che il record CNAME (per Easy DKIM) o il record TXT (per BYODKIM) utilizzi il nome corretto. Alcuni provider DNS aggiungono automaticamente il nome di dominio ai record creati. Ad esempio, se si crea un record con un nome di `example._domainkey.example.com`, il provider DNS potrebbe aggiungere il nome del dominio alla fine di questa stringa, con il risultato `example._domainkey.example.com.example.com`. Per ulteriori informazioni, consulta la documentazione fornita dal provider DNS.

Ricevi un'e-mail da Amazon SES che indica che la tua configurazione DKIM è stata (o sarà) revocata.

Ciò significa che Amazon SES non può più trovare i record CNAME richiesti (se si utilizza Easy DKIM) o il record TXT richiesto (se si utilizza BYODKIM) sul server DNS. L'e-mail di notifica comunica il tempo disponibile per pubblicare nuovamente i record DNS prima che lo stato della configurazione DKIM venga revocato e che la firma DKIM venga disabilitata. Se la configurazione DKIM viene revocata, è necessario riavviare la procedura di configurazione DKIM dall'inizio.

Quando si tenta di impostare BYODKIM, il processo di verifica DKIM ha esito negativo.

Assicurarsi che la chiave privata utilizzi il formato corretto. La chiave privata deve essere in formato PKCS #1 o PKCS #8 e utilizzare la crittografia RSA a 1024 o 2048 bit. Inoltre, la chiave privata deve essere codificata base64.

Durante l'impostazione di BYODKIM, viene visualizzato un errore **`BadRequestException`** quando si tenta di specificare una chiave pubblica per il dominio.

Se viene visualizzato un errore `BadRequestException`, effettuare le seguenti operazioni:

- Assicurarsi che il selettore specificato per la chiave pubblica contenga almeno un valore compreso tra 1 e 63 caratteri alfanumerici. Il selettore non può includere punti o altri simboli o punteggiatura.
- Assicurarsi di aver rimosso le righe di intestazione e piè di pagina dalla chiave pubblica e di aver rimosso tutte le interruzioni di riga dalla chiave pubblica.

Quando si utilizza Easy DKIM, i server DNS restituiscono i record CNAME DKIM Amazon SES, ma restituiscono **`SERVFAIL`** per il record TXT di verifica del dominio.

Il provider DNS potrebbe non essere in grado di reindirizzare i record CNAME. Amazon SES e ISP eseguono query per i record TXT. Per rispettare le specifiche DKIM, i tuoi server DNS devono essere in grado di rispondere alle query dei record TXT e dei record CNAME. Se il provider DNS non è in grado di rispondere alle query dei record TXT, un'alternativa è quella di utilizzare Route 53 come provider per l'hosting DNS.

Le tue email contengono due firme DKIM

La firma DKIM aggiuntiva, che contiene `d=amazonses.com`, viene aggiunta automaticamente da Amazon SES. Puoi ignorarla.

Problemi di recapito di Amazon SES

Quando si fa una richiesta ad Amazon SES, il messaggio spesso viene inviato immediatamente. In altri casi, è possibile che si verifichi un breve ritardo. In ogni caso esiste la certezza che l'e-mail verrà inviata.

Quando Amazon SES invia il messaggio, tuttavia, diversi fattori potrebbero impedirne il recapito e, in alcuni casi, ci si accorge che il recapito non è riuscito solo perché il messaggio inviato non arriva. Segui la procedura indicata di seguito per risolvere il problema.

Se un'e-mail non arriva, prova a eseguire le operazioni seguenti:

- Verifica di avere eseguito una richiesta `SendEmail` o `SendRawEmail` per l'e-mail in questione e di aver ricevuto una risposta di esito positivo. Se stai eseguendo queste richieste a livello di programmazione, controlla i registri del software per verificare che il programma abbia effettuato la richiesta e ricevuto una risposta di esito positivo.
- Leggi l'articolo del blog relativo alle tre posizioni in cui le e-mail inviate tramite SES potrebbero trovarsi, in quanto potrebbe trattarsi di un ritardo e non di un mancato recapito.
- Controlla l'indirizzo e-mail del mittente (indirizzo "From" (Da)) per verificare che sia valido. Controlla anche l'indirizzo del percorso di ritorno, ovvero quello a cui vengono inviati i messaggi con mancato recapito. Se l'e-mail è tornata al mittente, non sarà presente alcun messaggio di errore esplicativo.
- Controlla il Service Health Dashboard AWS per verificare che non si tratti di un problema noto con Amazon SES.
- Contatta il destinatario dell'e-mail o il rispettivo ISP. Verifica che il destinatario usi l'indirizzo e-mail corretto e se ci sono stati problemi di recapito noti con il rispettivo ISP. Accertati inoltre che l'e-mail sia arrivata ma sia stata filtrata come spam.
- Se ti sei registrato per un piano AWS Support a pagamento, puoi aprire una nuova richiesta di assistenza tecnica. Comunica gli indirizzi del destinatario rilevanti insieme a tutti gli ID della richiesta o del messaggio restituiti dalle risposte `SendEmail` o `SendRawEmail`.
- Attendi per vedere se si tratta di un ritardo e non di un errore di recapito permanente. Per combattere gli spammer, alcuni provider di servizi Internet rifiutano temporaneamente i messaggi in ingresso che provengono da server di posta elettronica sconosciuti. Questo processo, chiamato

greylisting, può causare un ritardo nel recapito. Amazon SES proverà di nuovo a inviare di questi messaggi. Se il problema è il greylisting, l'ISP potrebbe accettare l'e-mail durante uno di questi tentativi.

- Anche quando operi nell'interesse dei clienti è possibile che si verifichino situazioni che impattano sull'efficienza del recapito dei tuoi messaggi. Consulta the section called “Suggerimenti e best practice” per garantire che le tue comunicazioni e-mail raggiungano i destinatari previsti.

Problemi con le e-mail ricevute da Amazon SES

In questa sezione vengono descritti alcuni problemi comuni che potrebbero verificarsi quando si ricevono e-mail inviate da Amazon SES.

Il client e-mail visualizza "messaggio inviato via amazonses.com" come origine dell'e-mail

Alcuni client e-mail visualizzano il dominio "via" quando il dominio del mittente non corrisponde al dominio da cui è stata inviata l'e-mail (in questo caso, amazonses.com). Per ulteriori informazioni, consulta Informazioni aggiuntive accanto al nome del mittente sul sito Web del supporto di Gmail. In alternativa, puoi impostare DomainKeys Identified Mail (DKIM). Quando esegui l'autenticazione delle e-mail DKIM, i client e-mail di solito non mostrano il dominio "via" perché la firma DKIM dimostra che il mittente dell'e-mail è effettivamente il dominio dichiarato. Per informazioni sulla configurazione di DKIM, consulta Autenticazione delle e-mail con DKIM in Amazon SES.

> **Note**
>
> Se hai ricevuto spam o altri messaggi e-mail non richiesti da un utente SES, utilizza gli strumenti di segnalazione degli spam nel tuo client di posta elettronica e segui i passaggi per segnalare un uso illecito dell'e-mail SES elencato in Contattaci.

Il messaggio contiene caratteri confusi o privi di senso

Se il messaggio include caratteri non inclusi nel set di caratteri ASCII (ad esempio caratteri latini accentati, caratteri cinesi o caratteri arabi), devi codificare tali caratteri utilizzando la codifica dei caratteri HTML. Puoi utilizzare strumenti basati sul Web per codificare i caratteri nelle e-mail, ad esempio il Convertitore di caratteri HTML presente sul sito Email On Acid.

In alternativa, puoi assemblare manualmente il messaggio MIME. Nel messaggio MIME, puoi specificare che il messaggio deve utilizzare la codifica UTF-8. Quando utilizzi la codifica UTF-8,

puoi utilizzare caratteri non ASCII direttamente nei messaggi. Una volta completata la creazione del messaggio MIME, puoi inviarlo utilizzando l'API SendRawEmail o l'API SendMail v2.

Una causa comune di questo problema è la funzionalità Virgolette intelligenti di Microsoft Word. Se spesso copi dei contenuti da Word e li incolli nelle e-mail, è possibile che si verifichi questo problema. La funzionalità Virgolette intelligenti sostituisce i caratteri delle virgolette semplici ("...") con virgolette curve (“...”). I caratteri delle virgolette curve non sono caratteri ASCII standard. Di conseguenza, potrebbero essere renderizzati in alcuni client di posta elettronica come "??" o come gruppo di caratteri "â€". Per risolvere questo problema, puoi disattivare la funzionalità Virgolette intelligenti in Word. In alternativa, puoi utilizzare la soluzione SendRawEmail indicata nel paragrafo precedente. Per informazioni su come disattivare questa funzionalità, consulta Virgolette intelligenti in Word nel sito Web del supporto tecnico di Microsoft Office.

Problemi di notifica di Amazon SES

Di seguito sono elencate le possibili cause e soluzioni per eventuali problemi con le notifiche di mancato recapito, reclamo o recapito.

- Ricevi notifiche di mancato recapito tramite Amazon SNS, ma non sai a quali destinatari corrispondono; in futuro, per associare una notifica di mancato recapito a un determinato destinatario, hai a disposizione le seguenti opzioni:
  - Poiché Amazon SES non conserva gli ID messaggio personalizzati che aggiungi, archivia una mappatura tra un identificatore e l'ID messaggio Amazon SES che Amazon SES passa nuovamente a te quando accetta l'e-mail.
  - In ciascuna chiamata ad Amazon SES esegui l'invio a un singolo destinatario, anziché inviare un messaggio singolo a più destinatari.
  - Puoi abilitare un inoltro di feedback via e-mail, che inoltra a te il messaggio completo di mancato recapito.
- Ricevi notifiche di reclami o di consegna via Amazon SNS o inoltro di feedback via e-mail, ma non sai a quali destinatari corrispondono le notifiche. Alcuni ISP occultano l'indirizzo e-mail del destinatario del reclamo prima di trasferire la notifica ad Amazon SES. Il modo migliore per trovare l'indirizzo e-mail del destinatario è archiviare una mappatura propria tra un identificatore e l'ID messaggio Amazon SES che Amazon SES passa nuovamente a te quando accetta l'e-mail. Amazon SES non conserva gli ID messaggio personalizzati che aggiungi.
- Hai intenzione di configurare notifiche per accedere a un argomento Amazon SNS di cui non sei proprietario; il proprietario dell'argomento deve configurare una policy d'accesso Amazon SNS

che consenta al tuo account di chiamare l'operazione `SNS:Publish` sul suo argomento. Per informazioni su come controllare l'accesso al tuo argomento Amazon SNS utilizzando policy IAM, consulta la Gestione dell'accesso agli argomenti Amazon SNS nella Guida per gli sviluppatori di Amazon Simple Notification Service.

Errori di invio di e-mail con Amazon SES

In questo argomento vengono esaminati i tipi di errori specifici dell'invio di e-mail che potrebbero verificarsi quando si invia un'e-mail tramite Amazon SES. Se provi a inviare un'e-mail tramite Amazon SES e la chiamata ad Amazon SES non riesce, Amazon SES restituisce un messaggio di errore all'applicazione e non invia l'e-mail. Questo messaggio di errore varia in base al modo in cui si chiama Amazon SES.

- Se effettui una chiamata diretta all'API Amazon SES, l'operazione di query restituisce un errore. L'errore potrebbe essere `MessageRejected` o uno degli errori specificati nell'argomento Errori comuni della Documentazione di riferimento per le API di Amazon Simple Email Service.
- Se chiami Amazon SES utilizzando un SDK AWS che usa un linguaggio di programmazione che supporta le eccezioni, Amazon SES potrebbe generare un'eccezione. Il tipo di eccezione dipende dall'SDK e dall'errore. Ad esempio potrebbe essere un'eccezione `MessageRejectedException` di Amazon SES (il nome effettivo può variare in base all'SDK) o un'eccezione AWS generica. Indipendentemente dal tipo di eccezione, il tipo di errore e il messaggio di errore nell'eccezione forniscono ulteriori informazioni.
- Se chiami Amazon SES tramite l'interfaccia SMTP, il modo in cui si verifica l'errore dipende dall'applicazione. In alcune applicazioni potrebbe essere visualizzato un messaggio di errore specifico, mentre in altre no. Per l'elenco dei codici di risposta SMTP restituiti da Amazon SES, consulta Codici di risposta SMTP restituiti da Amazon SES.

> **Note**
>
> Quando la chiamata ad Amazon SES per l'invio di un'e-mail non riesce, l'e-mail non viene fatturata.

Di seguito sono elencati i tipi di problemi specifici di Amazon SES che possono comportare la restituzione di un errore da parte di Amazon SES quando provi a inviare un'e-mail. Questi errori si aggiungono agli errori generici di AWS come `MalformedQueryString`, come specificato

nell'argomento Errori comuni della Documentazione di riferimento per le API di Amazon Simple Email Service.

- Email address is not verified. The following identities failed the check in region region: identity1, identity2, identity3 (Le seguenti identità non hanno superato il controllo nella Regione <Regione>: <identità1>, <identità2>, <identità3>): stai provando a inviare l'e-mail da un indirizzo e-mail o un dominio che non hai verificato con Amazon SES. Questo errore potrebbe riguardare l'indirizzo "From" (Da), "Source" (Origine), "Sender" (Mittente) o "Return-Path" (Percorso di ritorno). Se il tuo account si trova ancora nella sandbox Amazon SES, devi verificare anche gli indirizzi e-mail di tutti i destinatari, ad eccezione dei destinatari forniti dal simulatore di mailbox Amazon SES. Se Amazon SES non è in grado di visualizzare tutte le identità che hanno determinato l'errore, il messaggio di errore termina con i puntini di sospensione.

  > **Note**
  >
  > Amazon SES dispone di endpoint in più Regioni AWS e lo stato della verifica degli indirizzi e-mail è separato per ciascuna Regione AWS. È necessario completare la procedura di verifica per ogni mittente nelle Regioni AWS che desideri utilizzare.

- Account is paused (Account sospeso): abbiamo sospeso la capacità del tuo account di inviare e-mail. È comunque possibile accedere alla console Amazon SES ed eseguire la maggior parte delle operazioni. Tuttavia, se tenti di inviare un'e-mail, riceverai questo messaggio.

  In caso di sospensione della capacità di inviare e-mail da parte del tuo account, inviamo automaticamente una notifica all'indirizzo e-mail associato al tuo Account AWS. Per ulteriori informazioni, consulta . the section called “Domande frequenti sul processo di verifica dell'invio”.

- Throttling (Limitazione): è possibile che l'applicazione stia provando a inviare un numero eccessivo di messaggi al secondo o che nelle ultime 24 ore sia stato inviato un numero eccessivo di e-mail. In questi casi, il messaggio di errore potrebbe somigliare agli esempi seguenti:
  - Daily message quota exceeded (Quota giornaliera messaggi superata): hai inviato il numero massimo di messaggi consentiti in un periodo di 24 ore. Se hai superato la quota giornaliera, dovrai attendere il successivo periodo di 24 ore prima di poter inviare altre e-mail.
  - Maximum sending rate exceeded (Frequenza massima in uscita superata): stai provando a inviare un numero maggiore di e-mail al secondo di quanto è consentito dalla frequenza massima in uscita. Se hai superato la frequenza di invio, puoi continuare a inviare e-mail ma devi ridurre la frequenza. Per ulteriori informazioni, consulta How to handle a "Throttling - Maximum sending rate exceeded" error nel blog AWS Messaging and Targeting.

- Maximum SigV2 SMTP sending rate exceeded (Velocità massima di invio SMTP SIGv2 superata): stai tentando di inviare messaggi utilizzando le credenziali SMTP create prima del 10 gennaio 2019; le credenziali SMTP sono state create utilizzando una versione precedente della firma AWS. Per motivi di sicurezza, devi eliminare le credenziali create prima di questa data e sostituirle con credenziali più recenti. Puoi eliminare le credenziali più vecchie usando la console IAM. Per ulteriori informazioni sulla creazione delle credenziali, consulta the section called “Richiesta delle credenziali SMTP”.

È opportuno monitorare regolarmente le attività di invio per vedere quanto manca al raggiungimento delle quote di invio. Per ulteriori informazioni, consulta . Monitoraggio delle quote di invio di Amazon SES. Per informazioni generali sulle quote di invio, consulta Gestione dei limiti di invio di Amazon SES. Per informazioni su come aumentare le quote di invio, consulta Aumento delle quote di invio di Amazon SES.

> **Important**
>
> Se il messaggio che spiega l'errore di throttling non è correlato al superamento della quota giornaliera o della frequenza massima in uscita, è possibile che esista un problema a livello di sistema che comporta una riduzione delle funzionalità di invio. Per informazioni sullo stato dei servizi, vai alla Service Health Dashboard di AWS.

- There are no recipients specified (Nessun destinatario specificato): non sono stati indicati i destinatari.
- There are non-ASCII characters in the email address (Nessun carattere non ASCII nell'indirizzo e-mail): la stringa dell'indirizzo e-mail deve essere ASCII a 7 bit. Se desideri utilizzare indirizzi e-mail (del mittente o del destinatario) che contengono caratteri Unicode nella parte del dominio, devi codificare il dominio utilizzando Punycode. Punycode non è consentito nella parte locale dell'indirizzo e-mail (ad esempio, la parte prima della @), né nel nome del mittente. Se desideri utilizzare caratteri Unicode nel nome del mittente, devi codificarlo con la sintassi MIME, come descritto in Invio di e-mail non elaborate utilizzando l'API Amazon SES v2. Per ulteriori informazioni su Punycode, consulta RFC 3492.
- Mail FROM domain is not verified (Dominio Mail FROM non verificato): Amazon SES non è riuscito a leggere il record MX necessario per usare il dominio MAIL FROM specificato. Per informazioni sulla configurazione di domini MAIL FROM personalizzati, consulta Uso di un dominio MAIL FROM personalizzato.

- Configuration set does not exist (Set di configurazione inesistente): il set di configurazione specificato non esiste. Un set di configurazione è un parametro opzionale che puoi utilizzare per pubblicare gli eventi di invio di e-mail. Per ulteriori informazioni, consulta . Monitoraggio dell'invio di e-mail utilizzando la pubblicazione di eventi di Amazon SES.

Aumento della velocità effettiva con Amazon SES

Quando invii e-mail, puoi effettuare chiamate ad Amazon SES con la frequenza consentita dalla frequenza massima in uscita. Per ulteriori informazioni sulla frequenza massima in uscita, consulta Gestione dei limiti di invio di Amazon SES. Tuttavia, ogni chiamata ad Amazon SES richiede tempo per il completamento.

Se esegui più chiamate ad Amazon SES utilizzando l'API Amazon SES o l'interfaccia SMTP, tieni presenti i seguenti suggerimenti utili per migliorare la velocità effettiva:

- Misura le tue prestazioni attuali per identificare i colli di bottiglia: un possibile test delle prestazioni implica l'invio di più e-mail il più rapidamente possibile all'interno di un loop di codice nell'applicazione. Misura la latenza del round trip di ogni richiesta `SendEmail`. Quindi, lancia istanze aggiuntive dell'applicazione in modo incrementale sullo stesso computer e osserva l'impatto sulla latenza di rete. Puoi eseguire il test anche su più computer e su reti diverse per individuare eventuali colli di bottiglia delle risorse dei computer o di rete esistenti.
- (Solo API) Usa le connessioni persistenti HTTP: per evitare di dover stabilire una nuova connessione HTTP separata per ogni richiesta API, è possibile usare le connessioni persistenti HTTP. Ciò significa che si può riutilizzare la stessa connessione HTTP per più richieste API.
- Usa più thread: quando un'applicazione usa un thread singolo, il codice dell'applicazione chiama l'API Amazon SES, quindi attende in modo sincrono una risposta dell'API. L'invio di e-mail in genere è un'operazione di I/O ed eseguire l lavoro da più thread garantisce una velocità effettiva migliore. Puoi fare invii simultanei utilizzando tutti i thread di esecuzione che desideri.
- Usa più processi: l'uso di più processi consente di aumentare la velocità effettiva in quanto sono presenti più connessioni attive simultanee ad Amazon SES. Ad esempio, puoi segmentare le e-mail in più bucket, quindi eseguire più istanze della tua e-mail inviando lo script contemporaneamente.
- Usa l'inoltro di e-mail locale: l'applicazione può trasmettere i messaggi rapidamente al server di posta locale, che può quindi aiutare a eseguire il buffering dei messaggi e a trasmetterli in modo asincrono ad Amazon SES. Alcuni server di posta supportano il recapito simultaneo, il che significa che anche se la tua applicazione genera e-mail per il server di posta con un unico thread, il server

utilizzerà più thread per l'invio ad Amazon SES. Per ulteriori informazioni, consulta Integrazione di Amazon SES con il server e-mail esistente.

- Ospita l'applicazione più in prossimità dell'endpoint dell'API Amazon SES: puoi ospitare la tua applicazione in un data center vicino all'endpoint dell'API Amazon SES o in un'istanza Amazon EC2 nella stessa Regione AWS dell'endpoint dell'API Amazon SES. Questo può aiutare a ridurre la latenza di rete tra l'applicazione e Amazon SES e a migliorare la velocità effettiva. Per un elenco di regioni in cui Amazon SES è disponibile, consulta Amazon Simple Email Service (Amazon SES) in Riferimenti generali di AWS.
- Usa più computer: a seconda della configurazione di sistema sul tuo computer host, potrebbe esserci un limite per il numero di connessioni HTTP simultanee a un solo indirizzo IP che può compromettere i vantaggi del parallelismo, una volta superato un determinato numero di connessioni simultanee su un singolo computer. Se si tratta di un collo di bottiglia, prova a eseguire richieste Amazon SES simultanee usando più computer.
- Usa l'API di query Amazon SES anziché l'endpoint SMTP: l'uso dell'API di query Amazon SES consente di inviare richieste di invio di e-mail con una sola chiamata di rete, mentre l'uso dell'endpoint SMTP comporta una conversazione SMTP costituita da più richieste di rete (ad esempio EHLO, MAIL FROM, RCPT TO, DATA, QUIT). Per ulteriori informazioni sull'API di query Amazon SES, consulta Utilizzo dell'API Amazon SES per l'invio di e-mail.
- Usa il simulatore di mailbox Amazon SES per testare la velocità effettiva massima: per testare le modifiche che è possibile implementare, puoi utilizzare il simulatore di mailbox. Il simulatore di mailbox può risultare utile per determinare la velocità effettiva massima del sistema senza usare tutta la quota di invio giornaliera. Per informazioni sul simulatore di mailbox, consulta Utilizzo manuale del simulatore di mailbox.

Se accedi ad Amazon SES tramite l'interfaccia SMTP, consulta Problemi relativi a SMTP in Amazon SES per i problemi specifici correlati a SMTP che possono influire sulla velocità effettiva.

Problemi relativi a SMTP in Amazon SES

Questa sezione contiene le soluzioni per diversi problemi comuni relativi all'invio di messaggi e-mail tramite l'interfaccia SMTP (Simple Mail Transfer Protocol) di Amazon SES. Contiene anche un elenco di codici di risposta SMTP restituiti da Amazon SES.

Per ulteriori informazioni sull'invio di messaggi e-mail tramite l'interfaccia SMTP di Amazon SES, consulta Utilizzo dell'interfaccia SMTP Amazon SES per inviare e-mail.

- Non riesci a connetterti all'endpoint SMTP Amazon SES.

  I problemi di connessione all'endpoint SMTP di Amazon SES sono molto spesso correlati ai problemi seguenti:

  - Credenziali errate: le credenziali utilizzate per connettersi all'endpoint SMTP sono diverse dalle credenziali dell'utente. AWS Per ottenere le credenziali SMTP, consulta Richiesta delle credenziali SMTP Amazon SES. Per ulteriori informazioni sulle credenziali, consulta Tipi di credenziali Amazon SES.
  - Problemi di rete o firewall: la rete potrebbe bloccare le connessioni in uscita sulla porta da cui stai provando a inviare e-mail. Per determinare se un problema di rete locale provoca problemi di connessione, digita il comando seguente sulla riga di comando, sostituendo *`port`* con la porta che stai provando a utilizzare (in genere 465, 587, 2465 o 2587): `telnet email-smtp.us-west-2.amazonaws.com` *`port`*

    Se riesci a connetterti al server SMTP utilizzando il comando e stai tentando di connetterti ad Amazon SES tramite TLS Wrapper o STARTTLS, completa le procedure illustrate in Verifica della connessione all'interfaccia SMTP Amazon SES utilizzando la riga di comando.

    Se non riesci a connetterti all'endpoint SMTP di Amazon SES utilizzando `telnet` o `openssl`, significa che un elemento in rete (ad esempio un firewall) blocca le connessioni in uscita sulla porta che stai provando a utilizzare. Collabora con l'amministratore di rete per diagnosticare e risolvere il problema.
- Stai inviando ad Amazon SES da un'istanza Amazon EC2 utilizzando la porta 25 e stai ricevendo degli errori di timeout.

  Amazon EC2 limita la porta 25 per impostazione predefinita. Per rimuovere queste restrizioni, invia una richiesta di rimozione dei limiti di invio di e-mail di Amazon EC2. Puoi anche connetterti ad Amazon SES utilizzando le porte 465 o 587 che non sono soggette a limitazioni.
- Errori di rete stanno causano la perdita di e-mail.

  Verifica che la tua applicazione utilizzi una logica di ripetizione quando si connette all'endpoint SMTP di Amazon SES e che sia in grado di rilevare e ripetere la consegna dei messaggi in caso di un errore di rete. Poiché SMTP è un protocollo di tipo verbose, l'invio di un'e-mail basato su di esso richiede diversi roundtrip. A causa della natura di SMTP, il potenziale per gli errori di rete aumenta.
- Perdi la connessione con l'endpoint SMTP.

  La perdita di connessione è molto spesso causata dai problemi seguenti:

- Dimensione dell'MTU: se ricevi un messaggio di errore di timeout, l'unità massima di trasmissione (MTU) dell'interfaccia di rete per il computer che usi per connetterti all'interfaccia SMTP di Amazon SES potrebbe essere troppo grande. Per risolvere questo problema, imposta la dimensione dell'MTU del computer su 1.500 byte.

  Per ulteriori informazioni su come impostare la dimensione dell'MTU sui sistemi operativi Windows, Linux e macOS, consulta l'argomento sulle Query bloccate nel client che non raggiungono il cluster nella Guida per la gestione di Amazon Redshift.

  Per ulteriori informazioni sull'impostazione della dimensione MTU per un'istanza Amazon EC2, consulta Network Maximum Transmission Unit (MTU) for Your EC2 Instance nella Amazon EC2 User Guide.

- Connessioni di lunga durata: l'endpoint SMTP di Amazon SES viene eseguito su un parco di istanze Amazon EC2 dietro un Elastic Load Balancer (ELB). Per garantire che il sistema sia tollerante ai guasti, up-to-date le istanze Amazon EC2 attive vengono periodicamente terminate e sostituite con nuove istanze. Poiché la tua applicazione si connette a un'istanza Amazon EC2 attraverso ELB, la connessione perde validità quando l'istanza Amazon EC2 viene terminata. È consigliabile stabilire una nuova connessione SMTP dopo aver consegnato un numero fisso di messaggi tramite un'unica connessione SMTP oppure se la connessione SMTP è rimasta attiva per un determinato periodo di tempo. Dovrai effettuare delle prove per individuare le soglie appropriate a seconda di dove è ospitata la tua applicazione e di come invia le e-mail ad Amazon SES.

- Vuoi conoscere gli indirizzi IP dei server di posta SMTP Amazon SES in modo da inserirli nella whitelist della tua rete.

  Gli indirizzi IP per gli endpoint SMTP di Amazon SES risiedono dietro i bilanciatori del carico. Di conseguenza, questi indirizzi IP cambiano frequentemente. Non è possibile fornire un elenco definitivo di tutti gli indirizzi IP per gli endpoint Amazon SES. Ti consigliamo di elencare il dominio `amazonses.com`, anziché consentire l'allowlisting di singoli indirizzi IP.

Codici di risposta SMTP restituiti da Amazon SES

Questa sezione contiene l'elenco dei codici di risposta SMTP restituiti dall'interfaccia SMTP di Amazon SES.

È consigliabile ritentare le richieste SMTP che ricevono errori 400. Ti consigliamo di implementare un sistema che ritenta le richieste con attese progressivamente più lunghe (ad esempio, attesa di

5 secondi prima di riprovare, quindi attesa di 10 secondi, quindi attesa di 30 secondi). Se il terzo tentativo non riesce, attendi 20 minuti e quindi ripeti il processo. Per visualizzare un esempio di un'implementazione che utilizza una policy di ripetizione esponenziale dei tentativi, consulta il post su Come gestire un errore "Throttling - Maximum sending rate exceeded" (superamento della frequenza massima in uscita con conseguente limitazione) nel Blog AWS Messaging and Targeting (Messaggistica e targeting AWS).

> **Note**
>
> AWS Gli SDK implementano automaticamente la logica di ripetizione, ma utilizzano l'interfaccia HTTPS anziché SMTP.

Se ricevi un errore 500, è necessario rivedere la richiesta per correggere un problema prima di inviare nuovamente la richiesta. Ad esempio, se le credenziali di AWS autenticazione non sono valide, devi aggiornare l'applicazione per utilizzare le credenziali corrette prima di inviare nuovamente la richiesta.

Descrizione	Codice di risposta	Ulteriori informazioni
Autenticazione riuscita	`235 Authentication successful`	Il client SMTP si è collegato e registrato al server SMTP.
Recapito riuscito	`250 Ok` *`MessageID`*	*`MessageID`* è un stringa di caratteri univoca utilizzata da Amazon SES per identificare un messaggio.
Servizio non disponibile	`421 Too many concurrent SMTP connections`	Amazon SES non è in grado di elaborare la richiesta perché attualmente ci sono troppe connessioni al server SMTP.
Errore di elaborazione locale	`451 Temporary service failure`	Amazon SES non è stato in grado di elaborare la richiesta. Potrebbero esserci problemi con la richiesta che ne impediscono l'elaborazione.

Descrizione	Codice di risposta	Ulteriori informazioni
Timeout	`451 Timeout waiting for data from client`	È trascorso troppo tempo tra le richieste, pertanto il server SMTP ha chiuso la connessione.
Quota di invio giornaliera superata	`454 Throttling failure: Daily message quota exceeded`	Hai superato il numero massimo di e-mail che Amazon SES consente di inviare in un periodo di 24 ore. Per ulteriori informazioni, consulta Gestione dei limiti di invio di Amazon SES.
Frequenza massima in uscita superata	`454 Throttling failure: Maximum sending rate exceeded`	Hai superato il numero massimo di e-mail che Amazon SES consente di inviare al secondo. Per ulteriori informazioni, consulta Gestione dei limiti di invio di Amazon SES.

Descrizione	Codice di risposta	Ulteriori informazioni
Problema di Amazon SES durante la convalida delle credenziali SMTP	`454 Temporary authentication failure`	Problemi che possono causare questo problema includono (a titolo esemplificativo): • Un problema con la crittografia tra l'applicazione di invio di e-mail e Amazon SES. È necessario utilizzare una connessione crittografata quando si esegue la connessione ad Amazon SES. Per ulteriori informazioni, consulta Connessione a un endpoint SMTP Amazon SES. • Un problema con Amazon SES. Controlla il Service Health Dashboard AWS per gli aggiornamenti.
Problema nel ricevere la richiesta	`454 Temporary service failure`	Amazon SES non ha ricevuto correttamente la richiesta. Di conseguenza, il messaggio non è stato inviato.
Credenziali errate	`530 Authentication required`	L'applicazione che utilizzi per inviare e-mail non tentato di autenticarsi quando si è connessa all'interfaccia SMTP di Amazon SES.

Descrizione	Codice di risposta	Ulteriori informazioni
Credenziali di autentica zione non valide	`535 Authentication Credentials Invalid`	L'applicazione utilizzata per inviare e-mail non ha specifica to le credenziali SMTP corrette ad Amazon SES. Tieni presente che le tue credenziali SMTP non sono le stesse delle tue credenziali. AWS Per ulteriori informazioni, consulta Richiesta delle credenziali SMTP Amazon SES.
Account non sottoscritto ad Amazon SES	`535 Account not subscribed to SES`	Il Account AWS proprietario delle credenziali SMTP non è registrato ad Amazon SES.
Il messaggio è troppo lungo	`552 Message is too long.`	Il messaggio che stai tentando di inviare supera la dimensione massima per i messaggi.
Account non sottoscritto ad Amazon SES	`535 Account not subscribed to SES`	Il Account AWS proprietario delle credenziali SMTP non è registrato ad Amazon SES.
Errore di sintassi MAIL FROM	`553 <email-address > Invalid email address`	È presente un errore di sintassi nella parte MAIL FROM del messaggio SMTP. Verificare di utilizzare il formato corretto e di non dimenticare di racchiudere l'indirizzo e-mail tra '<>'.
Errore di sintassi RCPT TO	`553 <email-address > address unknown`	È presente un errore di sintassi nella parte RCPT TO del messaggio SMTP. Verificare di utilizzare il formato corretto e di non dimenticare di racchiudere l'indirizzo e-mail tra '<>'.

Descrizione	Codice di risposta	Ulteriori informazioni
Utente non autorizzato a chiamare l'endpoint SMTP di Amazon SES	`554 Access denied: User` *`UserARN`* `is not authorized to perform ses:SendRawEmail on resource` *`IdentityARN`*	La policy AWS Identity and Access Management (IAM) o la politica di autorizzazione all'invio di Amazon SES dell'utente che possiede le credenziali SMTP non è autorizzata a chiamare l'endpoint SMTP di Amazon SES.

Descrizione	Codice di risposta	Ulteriori informazioni
Indirizzo e-mail non verificato	`554 Message rejected: Email address is not verified. The following identities failed the check in region` *`region`*`: `*`identity0`*` , `*`identity1`*` , `*`identity2`*	Stai cercando di inviare e-mail da un indirizzo e-mail o dominio che non è verificato per l'invio di e-mail dall'account Amazon SES. Questo errore potrebbe riguardare l'indirizzo "From" (Da), "Source" (Origine), "Sender" (Mittente) o "Return-Path" (Percorso di ritorno). Se l'account si trova ancora nella sandbox, devi verificare anche l'indirizzo e-mail di tutti i destinatari (ad eccezione dei destinatari forniti dal simulatore di mailbox Amazon SES). Se Amazon SES non è in grado di mostrare tutte le identità che non hanno superato il controllo di verifica, il messaggio di errore termina con tre punti (...). **Note** Amazon SES ha diversi Regioni AWS endpoint e lo stato di verifica dell'indirizzo e-mail è separato per ciascuno Regione AWS. Devi completare il processo di verifica per ogni mittente Regioni AWS che desideri utilizzare.

> **Note**
>
> Per i problemi SMTP che non vengono risolti dalla risoluzione dei problemi in questa pagina, prova le opzioni di supporto SES elencate in Contattaci.

Domande frequenti su Amazon SES

Questa sezione contiene le risposte a diverse domande frequenti relative all'utilizzo di Amazon SES.

Questa sezione contiene le domande frequenti relative agli argomenti seguenti:

- Domande frequenti sul processo di verifica dell'invio di Amazon SES
- Domande frequenti sulla DNS Blackhole List (DNSBL)
- Domande frequenti sui parametri per l'invio di e-mail con Amazon SES

Domande frequenti sul processo di verifica dell'invio di Amazon SES

Effettuiamo il monitoraggio delle e-mail inviate tramite Amazon SES per accertarci che il servizio non sia utilizzato per distribuire e-mail dannose, non richieste o di bassa qualità. Se notiamo che un utente invia contenuti che rientrano in una di queste categorie, eseguiamo delle azioni su quell'account. Questo processo è definito processo di verifica dell'invio.

In molti casi, quando rileviamo un problema con un account, mettiamo tale account in fase di verifica. In altri casi, interrompiamo la capacità di inviare e-mail dell'account. Adottiamo queste azioni per proteggere la reputazione del mittente di ciascun account e per evitare che altri utenti SES subiscano interruzioni del servizio e problemi di consegna.

Indice

Domande frequenti sulla fase di verifica dell'account

D1. Ho ricevuto un messaggio che indica che il mio account è in fase di verifica. Che cosa significa?

Abbiamo rilevato un problema relativo alle e-mail inviate dal tuo account e ti concediamo il tempo per risolverlo. Puoi continuare a inviare e-mail come faresti normalmente, ma devi anche correggere il problema che ci ha indotti a mettere il tuo account in fase di verifica. Se non correggi il problema prima del termine del periodo di revisione, potremmo sospendere la tua capacità di inviare ulteriori e-mail.

D2. Riceverò sempre una notifica se il mio account viene messo in fase di verifica?

Sì. Riceverai una notifica all'indirizzo e-mail associato al tuo account AWS .

D3. Perché non ho ricevuto una notifica circa il fatto che il mio account è in fase di verifica?

Quando il tuo account viene sottoposto a revisione, inviamo automaticamente un avviso all'indirizzo e-mail associato al tuo account. AWS Questo indirizzo email è quello che hai specificato al momento della creazione AWS dell'account. In alcuni casi, questo indirizzo e-mail può essere diverso da quello utilizzato per inviare e-mail tramite SES.

Ti consigliamo di monitorare la tua reputazione di mittente regolarmente consultando i parametri sulla reputazione. Puoi anche configurare allarmi automatici in Amazon CloudWatch. Questi allarmi possono inviarti una notifica quando i tuoi parametri di reputazione superano una determinata soglia. Puoi anche configurare Amazon in CloudWatch modo che ti contatti in altri modi, ad esempio inviando un messaggio di testo al tuo telefono cellulare.

D4. Il fatto che il mio account SES sia in fase di revisione influirà sul mio utilizzo di altri AWS servizi?

Potrai comunque utilizzare altri AWS servizi mentre il tuo account SES è in fase di revisione. Tuttavia, se richiedi un aumento della quota di servizio per un altro AWS servizio che invia comunicazioni in uscita (come Amazon SNS), tale richiesta potrebbe essere rifiutata fino alla fine del periodo di revisione per il tuo account SES.

D5. Cosa devo fare se il mio account è in fase di verifica?

Devi procedere in questo modo:

- Se la situazione lo permette, smetti di inviare e-mail finché non risolvi il problema. Puoi comunque inviare e-mail mentre il tuo account è in fase di verifica. Tuttavia, se scegli di continuare a inviare e-mail senza apportare modifiche, potresti inavvertitamente peggiorare il problema.
- Leggi l'e-mail che ti abbiamo inviato per ottenere un riepilogo del problema.
- Analizza le tue modalità di invio per determinare quale aspetto in particolare ha causato il problema.
- Dopo aver apportato modifiche che ritieni possano risolvere il problema, accedi alla AWS Console e vai al Support Center. Rispondi al caso che abbiamo aperto per tuo conto. Nel tuo messaggio, fornisci informazioni dettagliate sulle operazioni che hai effettuato per risolvere il problema e descrivi in che modo tali interventi potranno evitare che il problema si ripeta in futuro.
- Assicurati di fornire tutte le informazioni specifiche richieste. Abbiamo bisogno di queste informazioni per valutare la tua pratica.

D6. Come posso richiedere un riesame?

Puoi richiedere che esaminiamo la nostra decisione di sottoporre a revisione il tuo account. Per richiedere una revisione, accedi alla AWS console e vai al Support Center. Rispondi al caso che abbiamo aperto per tuo conto.

Nella tua richiesta, fornisci le informazioni che seguono:

- Informazioni sulla causa dell'evento in base al quale il tuo account è stato messo in fase di verifica.
- Un elenco delle modifiche apportate per risolvere il problema. Includi solo le operazioni che hai già implementato, non le operazioni che prevedi di implementare in futuro.
- Informazioni su come tali modifiche possono evitare che lo stesso problema si verifichi nuovamente in futuro.

A seconda del tipo di evento che ci ha indotti a porre il tuo account in fase di verifica, potremmo richiederti ulteriori informazioni. Consulta le domande frequenti relative al problema che hai riscontrato per un elenco delle informazioni che dovresti includere nella tua richiesta.

D7. Che cosa succede se la mia richiesta di riesame non viene accettata?

Risponderemo alla tua richiesta con informazioni sul motivo per cui tale richiesta non è stata accettata. In alcuni casi, potrai inviare un'altra richiesta se sei in grado di dimostrare che il problema è stato risolto e che le tue modifiche eviteranno che il problema si verifichi nuovamente in futuro.

D8. Potete aiutarmi a diagnosticare il problema?

In genere possiamo fornirti solo una panoramica generale del problema, informandoti, ad esempio, del fatto che il problema riguardi i mancati recapiti. Sarà tua responsabilità indagare sulla causa principale del problema.

D9. Come faccio a sapere se il mio account non è più in fase di verifica?

I parametri sulla reputazione includono informazioni relative allo stato corrente del tuo account. Per ulteriori informazioni, consulta Utilizzo dei parametri sulla reputazione per tenere traccia delle percentuali di mancati recapiti e reclami.

D10. Mettete il mio account in fase di verifica ogni volta che si verifica un problema?

No. In alcune situazioni, potremmo sospendere la capacità del tuo account di inviare e-mail senza prima mettere il tuo account in fase di verifica. Per esempio:

- se il problema è molto grave;
- se in passato il tuo account è stato messo in fase di verifica più volte per lo stesso problema. Per questo motivo, è importante risolvere il problema presente alla base anziché risolvere l'episodio specifico che ci hai indotti a mettere il tuo account in fase di verifica. Ad esempio, se una particolare campagna ci ha indotti a mettere il tuo account in fase di verifica, non puoi limitarti a interrompere tale campagna. Dovresti invece determinare quali proprietà della campagna sono problematiche e assicurarti di aver predisposto i processi necessari in modo che le campagne future non abbiano lo stesso problema.

In questi casi, ti invieremo automaticamente una notifica quando sospendiamo la capacità del tuo account di inviare e-mail.

D11. Che cosa succede se apporto le modifiche prima della scadenza del periodo di verifica?

Accedi a AWS Management Console e vai al Support Center. Rispondi al caso che abbiamo aperto per tuo conto. Nella tua risposta alla pratica, comunicaci di aver risolto il problema.

D12. Posso ricevere assistenza dal mio AWS rappresentante o dal Premium Support?

Se lavori già con un rappresentante AWS dell'account, lo contatteremo automaticamente quando il tuo account verrà sottoposto a revisione. Il rappresentante del tuo account potrebbe essere in grado

di fornire ulteriori informazioni per aiutarti a comprendere meglio il problema. Se utilizzi il servizio Premium Support, devi contattare il suddetto team per ulteriore assistenza.

Domande frequenti sulla sospensione dell'invio

D1. Ho ricevuto un messaggio che indica che la capacità del mio account di inviare e-mail è stata sospesa. Che cosa significa?

Abbiamo sospeso la capacità del tuo account di inviare e-mail a causa di un problema critico con le e-mail inviate. Nella maggior parte dei casi, sospendiamo gli account per uno dei motivi seguenti:

- Abbiamo precedentemente messo il tuo account in fase di verifica. I problemi che ci hanno indotti a mettere in fase di verifica il tuo account non sono stati risolti entro la fine del periodo di verifica, abbiamo così sospeso la capacità del tuo account di inviare e-mail.
- Abbiamo messo il tuo account in fase di verifica più volte per lo stesso problema.
- Le e-mail inviate dal tuo account hanno violato i Termini di servizio AWS. Qualora tali violazioni siano gravi, potremmo sospendere la capacità del tuo account di inviare e-mail senza prima mettere il tuo account in fase di verifica.

D2. Riceverò sempre una notifica quando la capacità del mio account di inviare e-mail viene sospesa?

Sì. Riceverai una notifica all'indirizzo e-mail associato al tuo account AWS .

D3. La capacità del mio account di inviare e-mail è stata sospesa. Perché non ho ricevuto una notifica?

In caso di sospensione della capacità di inviare e-mail da parte del tuo account, inviamo automaticamente una notifica all'indirizzo e-mail associato al tuo account.

> **Note**
>
> Quando crei il tuo AWS account, devi fornire un indirizzo e-mail. Puoi modificare questo indirizzo in qualsiasi momento. Per ulteriori informazioni sulla modifica dell'indirizzo associato al tuo AWS account, consulta Gestire un AWS account nella Guida per l'AWS Billing and Cost Management utente.

Puoi usare Amazon CloudWatch per creare allarmi che ti informano quando i tassi di rimbalzo e di reclami sono troppo alti. La creazione di un allarme è un buon metodo per ricevere un avviso anticipato circa quei fattori che possono indurci a sospendere la capacità del tuo account di inviare e-mail. Tuttavia, vi sono altri fattori, oltre ai mancati recapiti e ai reclami, che potrebbero indurci a sospendere la capacità di inviare e-mail. Per ulteriori informazioni sulla creazione di allarmi in, consulta. CloudWatch Creazione di allarmi di monitoraggio della reputazione tramite CloudWatch

Puoi anche utilizzare il Pannello di controllo degli account per determinare lo stato corrente del tuo account. Ad esempio, se la capacità del tuo account di inviare e-mail è attualmente sospesa, la sezione Stato account del Pannello di controllo dell'account visualizza lo stato di Sospeso. Se il tuo account è in grado di inviare e-mail normalmente, visualizza lo stato Healthy (Integro).

Infine, puoi controllare il AWS Health Dashboard (PHD) all'indirizzo https://phd.aws.amazon.com/ per determinare se la capacità del tuo account di inviare e-mail è attualmente sospesa. Quando sospendiamo la capacità di un account di inviare e-mail, aggiungiamo automaticamente un evento SES sending paused (Invio mediante SES sospeso) nella sezione Event log (Registro eventi) del PHD. L'evento SES sending paused (Invio mediante SES sospeso) ha sempre uno stato Closed (Chiuso), indipendentemente dal fatto che la capacità di inviare e-mail dell'account è attualmente sospesa. Il registro eventi include anche una copia dell'e-mail che abbiamo inviato all'indirizzo e-mail associato al tuo AWS account quando si è verificato l'evento di pausa dell'invio.

Puoi utilizzarlo CloudWatch per creare allarmi che ti avvisano quando compaiono nuovi eventi sulla tua Personal Health Dashboard. Per ulteriori informazioni, consulta Monitoraggio AWS Health degli eventi con CloudWatch eventi nella Guida per l'AWS Health utente.

D4. La capacità del mio account di inviare e-mail è stata sospesa. Ciò influisce sulla mia capacità di utilizzare altri AWS servizi?

Puoi comunque utilizzare altri AWS servizi mentre la capacità del tuo account di inviare e-mail è sospesa. Tuttavia, se richiedi un aumento della quota di servizio per un altro servizio AWS che invia comunicazioni in uscita (come ad esempio Amazon SNS), questa richiesta potrebbe essere rifiutata fino a quando non viene ripristinata la capacità del tuo account di inviare e-mail.

D5. Cosa devo fare la capacità del mio account di inviare e-mail viene sospesa?

Devi procedere in questo modo:

- Leggi l'e-mail che ti abbiamo inviato per ottenere un riepilogo del problema.

- Analizza le tue modalità di invio per determinare quale aspetto in particolare ha causato il problema.
- Dopo aver apportato modifiche che ritieni possano risolvere il problema, accedi alla AWS Console e vai al Support Center. Rispondi al caso che abbiamo aperto per tuo conto. Nel tuo messaggio, fornisci informazioni dettagliate sulle operazioni che hai effettuato per risolvere il problema e descrivi in che modo tali interventi potranno evitare che il problema si ripeta in futuro.
- Assicurati di fornire tutte le informazioni specifiche richieste. Abbiamo bisogno di queste informazioni per valutare la tua pratica.

D6. Cos'è un riesame?

Puoi richiederci di riesaminare la nostra decisione di porre il tuo account in fase di verifica. Consulta le seguenti domande per ulteriori informazioni su come richiedere un riesame.

D7. Come posso richiedere un riesame?

Per richiedere una revisione, accedi alla AWS console e vai al Support Center. Rispondi al caso che abbiamo aperto per tuo conto.

Nella tua richiesta, fornisci le informazioni che seguono:

- Informazioni sulla causa del problema.
- Un elenco delle modifiche apportate per risolvere il problema. Includi solo le operazioni che hai già implementato, non le operazioni che prevedi di implementare in futuro.
- Informazioni su come tali modifiche possono evitare che lo stesso problema si verifichi nuovamente in futuro.

A seconda del tipo di evento che ci ha indotti a sospendere la capacità del tuo account di inviare e-mail, potremmo richiederti ulteriori informazioni. Consulta le domande frequenti relative al problema che hai riscontrato per un elenco delle informazioni che dovresti includere nella tua richiesta.

D8. Che cosa succede se la mia richiesta non viene accettata?

Risponderemo alla tua richiesta con informazioni sul motivo per cui tale richiesta non è stata accettata. In alcuni casi, potrai inviare un'altra richiesta se sei in grado di dimostrare che il problema è stato risolto e che le tue modifiche eviteranno che il problema si verifichi nuovamente in futuro.

D9. Potete aiutarmi a diagnosticare il problema?

In genere possiamo fornirti solo una panoramica generale del problema, informandoti, ad esempio, del fatto che il problema riguardi i mancati recapiti. È tua responsabilità risolvere il problema.

D10. Come posso sapere se la capacità del mio account di inviare e-mail è stata ripristinata?

I parametri sulla reputazione includono informazioni relative allo stato corrente del tuo account. Per ulteriori informazioni, consulta Utilizzo dei parametri sulla reputazione per tenere traccia delle percentuali di mancati recapiti e reclami.

D11. Posso ricevere assistenza dal mio AWS rappresentante o dal Premium Support?

Se lavori già con un rappresentante AWS dell'account, lo contatteremo automaticamente se sospendiamo la capacità del tuo account di inviare e-mail. Il rappresentante del tuo account potrebbe essere in grado di fornire ulteriori informazioni per aiutarti a comprendere meglio il problema. Se utilizzi il servizio Premium Support, devi contattare il suddetto team per ulteriore assistenza.

Domande frequenti sui mancati recapiti

D1. Perché vi occupate dei mancati recapiti?

Le alte percentuali di mancato recapito vengono spesso utilizzate da entità quali provider di posta elettronica e organizzazioni antispam per rilevare mittenti che si impegnano in pratiche di invio di e-mail non corrette. Elevate percentuali di mancato recapito possono portare all'invio di e-mail alla cartella spam anziché alla posta in arrivo.

D2. Cosa devo fare se ricevo una notifica che indica che il mio account è in fase di verifica o che l'invio è stato sospeso a causa della percentuale di mancati recapiti del mio account?

Individua la causa del problema, quindi correggila. Dopo aver apportato modifiche che ritieni possano risolvere il problema, accedi alla AWS Console e vai al Support Center. Rispondi al caso che abbiamo aperto per tuo conto. Nel tuo messaggio, fornisci informazioni dettagliate sulle operazioni che hai effettuato per risolvere il problema e descrivi in che modo tali interventi potranno evitare che il problema si ripeta in futuro. Includi inoltre le seguenti informazioni:

- metodo usato per tenere traccia dei mancati recapiti;

- modo in cui verifichi la validità degli indirizzi e-mail dei nuovi destinatari prima di inviare loro e-mail. Ad esempio, quali dei consigli forniti in D11. Come posso ridurre al minimo i mancati recapiti? stai seguendo.

D3. Quali tipi di mancati recapiti vengono conteggiati rispetto alla percentuale di mancati recapiti?

La percentuale di mancati recapiti include solo i mancati recapiti permanenti verso domini che non hai verificato. I mancati recapiti permanenti, o hard bounce, sono errori di consegna permanenti, ad esempio un indirizzo inesistente. Gli errori temporanei e intermittenti come una mailbox piena o i mancati recapiti dovuti a indirizzi IP bloccati, non vengono conteggiati in relazione alla percentuale di mancati recapiti.

D4. Rendete note le percentuali di mancato recapito che potrebbero indurvi a mettere in fase di verifica il mio account o che potrebbero determinare la sospensione della capacità di inviare e-mail.

Per ottenere risultati ottimali, ti consigliamo di mantenere una percentuale di mancati recapiti inferiore al 2%. Percentuali di mancati recapiti superiori possono influire sulla consegna delle e-mail.

Se la percentuale di mancati recapiti è del 5% o superiore, l'account viene messo in fase di verifica. Se la percentuale di mancati recapiti è del 10% o superiore, la capacità dell'account di inviare ulteriori e-mail potrebbe essere sospesa finché il problema che ha causato l'elevata percentuale di mancati recapiti non è stato risolto.

D5. Per quale periodo di tempo viene calcolata la percentuale di mancati recapiti?

Non calcoliamo la percentuale di mancati recapiti secondo un periodo fisso di tempo, perché mittenti diversi inviano in base a percentuali diverse. Al contrario, analizziamo un volume rappresentativo, ossia un numero di e-mail che rappresenta la tua tipica prassi di invio. Per ottenere un risultato equo tra mittenti a volume elevato e a volume ridotto, il volume rappresentativo è diverso per ogni utente e cambia con il mutare dei pattern di invio dell'utente.

D6. Posso calcolare la mia frequenza di rimbalzo utilizzando le informazioni della console SES o dell' GetSendStatistics API?

La percentuale di mancati recapiti viene calcolata usando il volume rappresentativo; consulta D5. Per quale periodo di tempo viene calcolata la percentuale di mancati recapiti?. A seconda della frequenza

di invio, la frequenza di rimbalzo può andare più indietro nel tempo rispetto alla console SES o a quella recuperabile. `GetSendStatistics` Inoltre, nel calcolo della percentuale di mancati recapiti vengono considerate solo le e-mail inviate a domini non verificati. Tuttavia, se monitori regolarmente le percentuali di mancati recapiti tramite questi metodi, avrai comunque un buon indicatore da usare per individuare i problemi prima che i medesimi raggiungano un livello tale da indurci a mettere il tuo account in fase di verifica oppure tali da determinare la sospensione della capacità del tuo account di inviare e-mail.

D7. Come individuo gli indirizzi e-mail che provocano il mancato recapito?

Esamina le notifiche di rimbalzo inviate da SES. L'indirizzo e-mail a cui SES inoltra le notifiche dipende da come sono stati inviati i messaggi originali, come descritto in. Ricezione delle notifiche Amazon SES tramite e-mail Puoi anche configurare le notifiche di mancato recapito tramite Amazon Simple Notification Service (Amazon SNS), come descritto in Impostazione delle notifiche degli eventi per Amazon SES. Ricorda che la semplice rimozione degli indirizzi che causano il mancato recapito dalla lista di distribuzione senza ulteriori indagini può non essere sufficiente a risolvere il problema sottostante. Per informazioni su cosa fare per ridurre i mancati recapiti, consulta D11. Come posso ridurre al minimo i mancati recapiti?.

D8. Se non ho monitorato i mancati recapiti, potete fornirmi un elenco degli indirizzi che hanno causato il problema?

No, non siamo in grado di fornire un elenco completo degli indirizzi che hanno avuto dei mancati recapiti. È tua responsabilità monitorare e adottare misure in caso di mancati recapiti relativi al tuo account.

D9. Come devo gestire i mancati recapiti?

Devi rimuovere gli indirizzi che causano il mancato recapito dalla lista di distribuzione e smettere immediatamente di inviare e-mail a questi indirizzi. Se invii volumi ridotti di e-mail, può essere sufficiente monitorare i mancati recapiti via e-mail e rimuovere manualmente gli indirizzi che causano il problema dalla lista di distribuzione. Se il volume è maggiore, probabilmente dovrai configurare un processo automatico, elaborando a livello di programmazione la mailbox in cui ricevi i mancati recapiti o configurando notifiche di mancato recapito tramite Amazon SNS. Per ulteriori informazioni, consulta Impostazione delle notifiche degli eventi per Amazon SES.

D10. È possibile che il mancato recapito delle e-mail sia dovuto al fatto che ho raggiunto la quota di invio?

No. I mancati recapiti non sono correlati alle quote di invio. Se tenti di superare la quota di invio, riceverai un errore dall'API SES o dall'interfaccia SMTP quando tenti di inviare un'e-mail.

D11. Come posso ridurre al minimo i mancati recapiti?

Prima di tutto, devi essere a conoscenza dei mancati recapiti; consulta D7. Come individuo gli indirizzi e-mail che provocano il mancato recapito?. Segui quindi queste linee guida:

- Non acquistare, noleggiare o condividere indirizzi e-mail. Invia e-mail solo ai destinatari che hanno esplicitamente richiesto di ricevere e-mail da parte tua.
- Rimuovi gli indirizzi e-mail che causano il mancato recapito dalla lista di distribuzione.
- Nei moduli Web, chiedi agli utenti di immettere il loro indirizzo e-mail due volte e verifica che entrambi gli indirizzi corrispondano prima che il modulo possa essere inviato.
- Usa l'opzione di doppio consenso esplicito per registrare nuovi utenti. Ovvero, quando nuovi utenti si registrano, invia loro un'e-mail di conferma su cui devono fare clic prima di poter ricevere altre e-mail. In questo modo, impedirai agli utenti di registrare altre persone ed eviterai registrazioni accidentali.
- Se devi inviare e-mail a indirizzi cui non hai inviato posta di recente e, di conseguenza, non hai la certezza che siano ancora validi, fallo solo con una piccola parte del volume di invio complessivo. Per ulteriori informazioni, consulta il nostro post di blog su cosa fare se è necessario inviare e-mail a vecchi indirizzi.
- Evita di strutturare le registrazioni in modo da incoraggiare gli utenti a usare indirizzi fittizi. Ad esempio, non offrire alcun valore aggiunto o beneficio finché i destinatari non verificano i loro indirizzi.
- Se hai impostato una funzionalità di invio a un amico, assicurati di usare un CAPTCHA o un meccanismo simile per scoraggiare l'uso automatico di questa funzionalità e non consentire l'inserimento di contenuto arbitrario da parte dell'utente.
- Se utilizzi SES per le notifiche di sistema, assicurati di inviarle a indirizzi reali che possono ricevere posta. Valuta anche se disattivare le notifiche non necessarie.
- Se stai testando un nuovo sistema, assicurati di inviarlo a indirizzi reali in grado di ricevere e-mail oppure di utilizzare il simulatore di caselle di posta SES. Per ulteriori informazioni, consulta Utilizzo manuale del simulatore di mailbox.

Domande frequenti sui reclami

D1. Cos'è un reclamo?

Un reclamo avviene quando un destinatario segnala che non vuole ricevere un'e-mail. Potrebbero aver fatto clic sul pulsante «Segnala spam» nel proprio client di posta elettronica, aver inoltrato un reclamo al proprio provider di posta elettronica, notificato direttamente SES o tramite un altro metodo. Questo argomento include informazioni generali sui reclami. Se la notifica contiene informazioni specifiche sull'origine dei reclami, leggi anche l'argomento pertinente:

- Domande frequenti sui reclami SES tramite i circuiti di feedback
- Domande frequenti sui reclami SES direttamente dai destinatari
- Domande frequenti sui reclami SES tramite provider di posta elettronica

D2. Perché vi occupate dei reclami?

Percentuali elevate di reclami vengono spesso usate da entità come i provider di posta elettronica e organizzazioni antispam come indicatori del fatto che un mittente invia e-mail a destinatari che non si sono espressamente registrati per la ricezione di e-mail o che il mittente sta inviando contenuto diverso dal tipo per il quale i destinatari si sono registrati.

D3. Cosa devo fare se ricevo una notifica indicante che il mio account è in fase di verifica o che l'invio è stato sospeso a causa di un problema con i reclami?

Inizia verificando il processo di acquisizione delle liste di distribuzione e il contenuto delle e-mail per identificare i motivi per cui i destinatari possono non gradire le tue e-mail. Individua la causa del problema, quindi correggila. Dopo aver apportato modifiche che ritieni possano risolvere il problema, accedi alla AWS Console e vai al Support Center. Rispondi al caso che abbiamo aperto per tuo conto. Nel tuo messaggio, fornisci informazioni dettagliate sulle operazioni che hai effettuato per risolvere il problema e descrivi in che modo tali interventi potranno evitare che il problema si ripeta in futuro.

D4. Come posso ridurre al minimo i reclami?

Innanzitutto, assicurati di monitorare i reclami che SES può segnalarti, ossia i reclami che SES riceve tramite cicli di feedback (consulta laDomande frequenti sui reclami SES tramite i circuiti di feedback). Segui quindi queste linee guida:

- Non acquistare, noleggiare o condividere indirizzi e-mail. Usa solo gli indirizzi che hanno espressamente richiesto di ricevere posta da te.
- Usa l'opzione di doppio consenso esplicito per registrare nuovi utenti. In altre parole, quando gli utenti si registrano, invia loro un'e-mail di conferma su cui devono fare clic prima di poter ricevere altre e-mail. In questo modo, impedirai agli utenti di registrare altre persone ed eviterai registrazioni accidentali.
- Monitora l'interazione degli utenti con la posta che invii e smetti di inviare e-mail ai destinatari che non fanno clic sui tuoi messaggi o che non li aprono.
- Quando nuovi utenti si registrano, descrivi con chiarezza il tipo di e-mail che riceveranno e assicurati di inviare solo il tipo di e-mail per cui si sono registrati. Ad esempio, se gli utenti si registrano per aggiornamenti sulle notizie, non inviare loro annunci pubblicitari.
- Assicurati che i messaggi siano ben formattati e abbiano un aspetto professionale.
- Assicurati di indicare con chiarezza che i messaggi provengono da te e che non possano essere confusi con qualcos'altro.
- Fornisci agli utenti un modo chiaro e semplice per annullare la sottoscrizione dei tuoi messaggi.

Domande frequenti sui reclami SES tramite i circuiti di feedback

Questo argomento fornisce informazioni sui reclami che SES riceve dai provider di posta elettronica tramite circuiti di feedback. Per informazioni generali valide per tutti i tipi di reclami, consulta Domande frequenti sui reclami.

D1. Come viene segnalato questo tipo di reclamo?

La maggior parte dei programmi client di posta elettronica offre la possibilità di classificare le e-mail come "spam" mediante un pulsante che consente di spostare il messaggio in una cartella spam e di inoltrarlo al provider di posta elettronica. Inoltre, la maggior parte dei provider di posta elettronica ha un indirizzo per l'uso illecito, ad esempio abuse@example.com, al quale gli utenti possono inoltrare le e-mail indesiderate e richiedere al provider di intervenire per impedirne l'invio. Se SES ha impostato un feedback loop (FBL) con il provider di posta elettronica, invia il reclamo a SES.

> **Note**
>
> SES imposta automaticamente l'intestazione Feedback-ID quando si inviano messaggi, offrendo ai provider di caselle di posta un modo per aggregare le statistiche di consegna, come le percentuali di reclami e spam, e renderle disponibili all'utente. Il valore dell'intestazione Feedback-ID fornito da SES è così composto:

- `FeedBackId:((SESInternalID):(AmazonSES))`, dove:
  - SESInternalID è l'identificatore utilizzato da SES per raccogliere informazioni sui reclami.
  - AmazonSES è un tag statico che identifica SES come piattaforma di invio.

Facoltativamente, oltre al valore di intestazione Feedback-ID standard fornito da SES, puoi anche specificare i tuoi ID di feedback personalizzati (fino a due) utilizzando i tag e message, vedi. `ses:feedback-id-a` `ses:feedback-id-b` the section called “Feedback dettagliato per le campagne e-mail”

D2. Questi reclami sono inclusi nella statistica sul tasso di reclami mostrata nella console SES e restituita dall'API? GetSendStatistics

Sì. Tuttavia, la statistica sul tasso di reclami non include i reclami dei provider di posta elettronica che non forniscono feedback a SES. La percentuale di reclami dai domini che forniscono feedback sarà probabilmente rappresentativa dell'invio generale.

D3. Come mi vengono notificati questi reclami?

Puoi ricevere notifiche via e-mail o tramite Amazon SNS. Consulta le istruzioni di configurazione in Impostazione delle notifiche degli eventi per Amazon SES.

D4. Cosa devo fare se ricevo una notifica di reclamo via e-mail o tramite Amazon SNS?

Prima di tutto, devi rimuovere gli indirizzi che hanno generato i reclami dalla lista di distribuzione e smettere immediatamente di inviare posta a questi indirizzi. Evita di inviare anche un'e-mail per informare gli utenti che hai ricevuto la richiesta di annullamento della sottoscrizione. Valuta di configurare un processo automatico, elaborando a livello di programmazione la mailbox in cui ricevi i reclami o configurando notifiche di reclamo tramite Amazon SNS. Per ulteriori informazioni, consulta Impostazione delle notifiche degli eventi per Amazon SES.

Esamina quindi più attentamente i tuoi criteri di invio per determinare perché i destinatari non gradiscono i messaggi che invii loro e cerca di risolvere questo problema sottostante. Per ogni persona che invia un reclamo, esistono potenzialmente decine di utenti che non gradiscono i messaggi ma che non hanno reclamato (o non sono stati in grado di reclamare). Se ti limiti a rimuovere i destinatari che hanno effettivamente inviato il reclamo, non risolvi il problema sottostante.

D5. Comunicate le percentuali di reclami di SES che potrebbero causare la messa in fase di revisione del mio account o che potrebbero mettere in pausa la capacità del mio account di inviare e-mail?

Per ottenere risultati ottimali, ti consigliamo di mantenere una percentuale di reclami inferiore allo 0,1%. Percentuali di reclami superiori possono influire sulla consegna delle e-mail.

Se la percentuale di reclami è dello 0,1% o superiore, l'account viene messo in fase di verifica. Se la percentuale di reclami è dello 0,5% o superiore, la capacità dell'account di inviare ulteriori e-mail potrebbe essere sospesa finché il problema che ha causato l'elevata percentuale di reclami non è stato risolto.

D6. Per quale periodo di tempo viene calcolata la percentuale di reclami?

Non calcoliamo la percentuale di reclami secondo un periodo fisso di tempo, perché mittenti diversi inviano in base a percentuali diverse. Al contrario, analizziamo un volume rappresentativo, ossia un numero di e-mail che rappresenta la tua tipica prassi di invio. Per ottenere un risultato equo tra mittenti a volume elevato e a volume ridotto, il volume rappresentativo è diverso per ogni utente e cambia con il mutare dei pattern di invio dell'utente. Inoltre, la percentuale di reclami non viene calcolata in base a ogni e-mail. Viene invece calcolata come percentuale di reclami relativi alla posta inviata a domini che inviano feedback sui reclami a SES.

D7. Posso calcolare la mia percentuale di reclami utilizzando le metriche della console SES o dell' GetSendStatisticsAPI?

No. I motivi principali sono due:

- La percentuale di reclami viene calcolata usando il volume rappresentativo. Consulta D6. Per quale periodo di tempo viene calcolata la percentuale di reclami?. A seconda della frequenza di invio, la percentuale di reclami può andare più indietro nel tempo rispetto a quella recuperata dalla console o dall'`GetSendStatistics`API SES. Per questo motivo, ti consigliamo di utilizzare questi metodi per monitorare regolarmente la percentuale di reclami per il tuo account. In questo modo, il monitoraggio della percentuale di reclami ti offre le informazioni di cui hai bisogno per identificare i problemi prima di raggiungere livelli che possono inficiare la consegna delle tue e-mail.
- Il calcolo della percentuale di reclami non conteggia ogni e-mail. La percentuale di reclami viene calcolata come percentuale di reclami relativi alla posta inviata a domini che inviano feedback sui reclami a SES.

D8. Come individuo gli indirizzi e-mail che hanno inviato reclami?

Esamina le notifiche di reclamo che SES ti invia tramite e-mail o Amazon SNS (vediImpostazione delle notifiche degli eventi per Amazon SES). Tuttavia, diversi provider di posta elettronica forniscono quantità diverse di informazioni e alcuni provider oscurano l'indirizzo e-mail del destinatario prima di inviare la notifica di reclamo a SES. Per consentirvi di trovare l'indirizzo e-mail del destinatario in futuro, l'opzione migliore è quella di memorizzare la vostra mappatura tra un identificatore e l'ID del messaggio SES che SES vi restituisce quando accetta l'e-mail. Tieni presente che SES non conserva gli ID dei messaggi personalizzati che aggiungi.

D9. Se non ho monitorato i reclami, potete fornirmi un elenco degli indirizzi che hanno inviato un reclamo?

Sfortunatamente non possiamo fornirti un elenco completo. Tuttavia, puoi monitorare i futuri reclami via e-mail o tramite Amazon SNS.

D10. Posso ricevere un'e-mail di esempio?

Non possiamo inviarti un'e-mail di esempio su richiesta, ma puoi trovare queste informazioni nella notifica di reclamo. Per ulteriori informazioni, consulta D8. Come individuo gli indirizzi e-mail che hanno inviato reclami?.

Domande frequenti sui reclami SES direttamente dai destinatari

Questo argomento fornisce informazioni sui reclami che SES riceve direttamente dai destinatari. Per informazioni generali valide per tutti i tipi di reclami, consulta Domande frequenti sui reclami.

D1. Come viene segnalato questo tipo di reclamo?

Più destinatari hanno contattato direttamente SES in merito alla posta dell'utente tramite e-mail o altri mezzi.

D2. Questi reclami sono inclusi nella statistica sul tasso di reclami mostrata nella console SES e restituita dall' GetSendStatistics API?

No. La statistica sulla percentuale di reclami recuperata utilizzando la console SES o l'`GetSendStatistics`API include solo i reclami che SES riceve tramite cicli di feedback. Per ulteriori informazioni su questi tipi di reclami, consulta Domande frequenti sui reclami SES tramite i circuiti di feedback.

D3. Perché non ho ricevuto informazioni su questi reclami tramite notifiche di feedback via e-mail o Amazon SNS?

L'inoltro di feedback via e-mail e le notifiche di Amazon SNS includono solo i reclami ricevuti da SES tramite cicli di feedback. Non riceverai notifiche relative ai reclami che i destinatari hanno presentato direttamente a SES.

D4. Come individuo gli indirizzi e-mail che hanno inviato reclami?

Per proteggere le identità dei destinatari che effettuano reclami, non possiamo elencare gli indirizzi e-mail che effettuano reclami in relazione alle tue e-mail.

Invece di concentrarti sulla rimozione di singoli destinatari dai tuoi elenchi, ti consigliamo di individuare il problema che ha generato i reclami. Ti consigliamo di iniziare rivedendo il processo di acquisizione dei clienti e di rimuovere dai tuoi elenchi i clienti che non hanno chiesto esplicitamente di ricevere e-mail da parte tua. Dovresti inoltre analizzare i contenuti delle e-mail per cercare di comprendere perché i destinatari hanno effettuato dei reclami.

D5. Posso ricevere un'e-mail di esempio?

Per proteggere le identità dei destinatari che effettuano reclami, non possiamo fornire copie delle e-mail che hanno causato dei reclami da parte dei tuoi destinatari.

D6. Cosa devo fare se ricevo una notifica indicante che il mio account è in fase di verifica o che l'invio è stato sospeso a causa di reclami diretti?

Modifica immediatamente i tuoi processi di invio in modo da inviare messaggi solo ai destinatari che hanno specificamente scelto di riceverli. Inoltre, accertarti di inviare il tipo di contenuto per il quale i destinatari si sono registrati. Dopo aver apportato modifiche che ritieni possano risolvere il problema, accedi alla AWS Console e vai al Support Center. Rispondi al caso che abbiamo aperto per tuo conto. Nel tuo messaggio, fornisci informazioni dettagliate sulle operazioni che hai effettuato per risolvere il problema e descrivi in che modo tali interventi potranno evitare che il problema si ripeta in futuro.

Se non richiedi una verifica entro tre settimane e continui a ricevere dei reclami diretti da parte dei destinatari, potremmo sospendere la capacità del tuo account di inviare e-mail.

Domande frequenti sui reclami SES tramite provider di posta elettronica

Questo argomento fornisce informazioni sui reclami che SES riceve tramite provider di posta elettronica (detti anche provider di cassette postali). Per informazioni generali valide per tutti i tipi di reclami, consulta Domande frequenti sui reclami.

D1. Come viene segnalato questo tipo di reclamo?

Un provider di posta elettronica ha segnalato a SES che un numero significativo di clienti ha contrassegnato le tue e-mail come spam. Il rapporto è stato fornito a SES con un mezzo diverso dai circuiti di feedback descritti nelDomande frequenti sui reclami SES tramite i circuiti di feedback.

D2. Questi reclami sono inclusi nella statistica sul tasso di reclami mostrata nella console SES e restituita dall' GetSendStatistics API?

No. La statistica sulla percentuale di reclami recuperata utilizzando la console SES o l'`GetSendStatistics`API include solo i reclami che SES riceve tramite cicli di feedback.

D3. Perché non ho ricevuto informazioni su questi reclami tramite notifiche di feedback via e-mail o Amazon SNS?

L'inoltro di feedback via e-mail e le notifiche di Amazon SNS includono solo i reclami ricevuti da SES tramite cicli di feedback.

D4. Come individuo gli indirizzi e-mail che hanno inviato reclami?

I provider di posta elettronica, in genere, non divulgano queste informazioni. Tuttavia, invece di concentrarti sulla rimozione di singoli destinatari dalla lista di distribuzione, devi trovare e risolvere il problema sottostante. Inizia esaminando il processo di acquisizione delle liste di distribuzione e il contenuto delle e-mail per identificare i motivi per cui i destinatari possono non gradire le tue e-mail.

D5. Posso ricevere un'e-mail di esempio?

No. I provider di posta elettronica in genere non forniscono un'e-mail di esempio.

D6. Cosa devo fare se ricevo una notifica indicante che il mio account è in fase di verifica o che l'invio è stato sospeso a causa di reclami dei provider di posta elettronica?

Individua la causa del problema, quindi correggila. Dopo aver apportato modifiche che ritieni possano risolvere il problema, accedi alla AWS Console e vai al Support Center. Rispondi al caso che

abbiamo aperto per tuo conto. Nel tuo messaggio, fornisci informazioni dettagliate sulle operazioni che hai effettuato per risolvere il problema e descrivi in che modo tali interventi potranno evitare che il problema si ripeta in futuro. Se non richiedi una verifica entro tre settimane e continui a ricevere dei reclami da parte dei provider, potremmo sospendere la capacità del tuo account di inviare ulteriori e-mail.

Domande frequenti sugli indirizzi spamtrap

D1. Cosa sono gli spamtrap?

Un indirizzo spamtrap è un indirizzo e-mail speciale gestito da un fornitore di servizi Internet (ISP), un provider di posta elettronica o un'organizzazione antispam. Poiché questo indirizzo non può mai essere legittimamente registrato per la ricezione di e-mail, le organizzazioni che gestiscono gli indirizzi spamtrap sanno che chiunque invii posta a tali indirizzi usa probabilmente criteri di invio di e-mail discutibili.

D2. Come si configurano gli spamtrap?

Gli indirizzi spamtrap possono essere configurati in più modi. Possono essere convertiti da indirizzi precedentemente validi, ma che sono rimasti inutilizzati e che hanno causato il mancato recapito per un periodo di tempo prolungato. Possono inoltre essere indirizzi configurati appositamente come spamtrap. Possono essere indirizzi insoliti difficili da indovinare e a volte sono indirizzi simili a indirizzi reali, in cui ad esempio è stato introdotto un errore di digitazione in un nome di dominio comune. Spesso, ma non sempre, gli spamtrap vengono introdotti nel mondo reale presentandoli in Internet in diversi modi.

D3. Come fa SES a sapere se sto inviando messaggi a spamtraps?

Alcune organizzazioni che utilizzano spamtrap inviano notifiche SES quando le loro trappole di spam vengono colpite da mittenti SES.

D4. In che modo SES utilizza i report spamtrap?

Verifichiamo i report. Se notiamo che il tuo account invia e-mail agli indirizzi spamtrap, mettiamo il tuo account in fase di verifica e ti chiediamo di risolvere il problema sottostante. Se non correggi il problema prima del termine del periodo di verifica, potremmo sospendere la tua capacità di inviare ulteriori e-mail. Se il problema con gli indirizzi spamtrap è molto grave, potremmo sospendere immediatamente la capacità del tuo account di inviare e-mail, senza mettere prima il tuo account in fase di verifica.

D5. Cosa devo fare se ricevo una notifica indicante che il mio account è in fase di verifica o che l'invio è stato sospeso a causa di un problema con gli indirizzi spamtrap?

In primo luogo, devi risolvere il problema che ci ha indotti a mettere il tuo account in fase di verifica o che ha determinato la sospensione della capacità di inviare e-mail. Successivamente, accedi alla AWS console e vai al Support Center. Rispondi al caso che abbiamo aperto per tuo conto. Nel tuo messaggio, fornisci informazioni dettagliate sulle operazioni che hai effettuato per risolvere il problema e descrivi in che modo tali interventi potranno evitare che il problema si ripeta in futuro. Se riteniamo che le modifiche apportate possono risolvere in modo appropriato il problema, annulliamo il periodo di verifica o la sospensione dell'invio del tuo account.

In virtù del modo in cui sono riportati gli eventi spamtrap, potrebbero essere necessarie tre settimane o un periodo più lungo per determinare se le modifiche apportate hanno risolto problema.

D6. Quanti eventi spamtrap possono verificarsi prima che il mio account venga posto in fase di verifica o prima che venga sospesa la capacità del mio account di inviare e-mail?

Non comunichiamo il numero specifico di eventi spamtrap che ci portano a intervenire sul tuo account. Tuttavia, è importante notare che anche un piccolo numero di eventi spamtrap può avere un effetto molto negativo sulla tua reputazione di mittente, pertanto dovresti prestare grande attenzione ai report relativi agli indirizzi spamtrap.

D7. Rendete noti gli indirizzi spamtrap?

No. Affinché gli indirizzi spamtrap siano efficaci, è fondamentale mantenere riservate queste informazioni. Le organizzazioni che usano spamtrap rendono noto solo il numero di invii a indirizzi spamtrap e non gli effettivi indirizzi.

D8. Come posso evitare di inviare e-mail a indirizzi spamtrap?

Per ridurre il rischio di inviare e-mail a indirizzi spamtrap, segui queste linee guida:

- Non acquistare, noleggiare o condividere indirizzi e-mail. Usa solo gli indirizzi che hanno espressamente richiesto di ricevere posta da te.
- Nei moduli Web, chiedi agli utenti di immettere il loro indirizzo e-mail due volte e verifica che entrambi gli indirizzi corrispondano prima che il modulo possa essere inviato.

- Usa l'opzione di doppio consenso esplicito per registrare nuovi utenti. In altre parole, quando gli utenti si registrano, invia loro un'e-mail di conferma su cui devono fare clic prima di poter ricevere altre e-mail.
- Assicurati di eliminare gli indirizzi che hanno causato mancati recapiti permanenti dalla tua lista di distribuzione, in modo da rimuoverli ben prima che vengano convertiti in spamtrap.
- Assicurati di monitorare l'interazione da parte dei destinatari e smetti di inviare e-mail a destinatari che non hanno interagito con le tue e-mail o i tuoi siti Web di recente. Gli intervalli di tempo che determinano che un utente interagisce con la tua posta dipendono dal tuo caso d'uso, ma in genere se gli utenti non hanno fatto clic sulle tue e-mail né le hanno aperte per diversi mesi, devi prendere in considerazione di rimuovere questi indirizzi a meno che non hai prove concrete del fatto che questi utenti desiderano ricevere le tue e-mail.
- Presta molta attenzione alle campagne di coinvolgimento in cui contatti intenzionalmente le persone che non hanno interagito con te di recente. Questi tentativi tendono a essere notevolmente rischiosi e spesso possono causare problemi non solo relativi all'invio a indirizzi spamtrap, ma anche ai mancati recapiti e ai reclami.
- Invia un messaggio per il consenso esplicito all'intera lista di distribuzione e mantieni solo i destinatari che fanno clic sul collegamento di verifica. Oltre a eliminare i destinatari non attivi dalla lista, questa procedura aiuta anche a rimuovere gli indirizzi spamtrap. Tuttavia, ti consigliamo di non usare questa tecnica se ritieni che la mailing list possa contenere molti indirizzi non validi o se il tuo account ha già un problema relativo ai mancati recapiti, perché in questo caso la percentuale di mancati recapiti potrebbe aumentare ulteriormente.

Domande frequenti sulle verifiche manuali

D1. Cosa devo fare se ricevo una notifica indicante che il mio account è in fase di verifica o che l'invio è stato sospeso a causa di una verifica manuale?

Un investigatore SES ha identificato un problema significativo relativo al tuo invio. I problemi più frequenti includono, a titolo esemplificativo, quanto segue:

- Le tue procedure di invio violano le policy di uso accettabile di AWS.
- Le tue e-mail sembrano essere considerate indesiderate.
- I tuoi contenuti sono correlati al phishing (incluso il phishing simulato).
- I tuoi contenuti sono altrimenti associati a un caso d'uso non supportato da SES.

Se riteniamo che il problema può essere corretto, mettiamo il tuo account in fase di verifica per un determinato periodo di tempo. Mentre il tuo account è in fase di verifica, dovresti modificare le tue pratiche di invio delle e-mail per risolvere il problema.

Se riteniamo che il problema non può essere corretto, oppure se il problema è molto grave, potremmo sospendere la capacità del tuo account di inviare e-mail senza mettere prima il tuo account in fase di verifica.

D2. Quali problemi potrebbero determinare l'esecuzione di una verifica manuale in relazione al mio invio di e-mail?

Vi sono diversi i problemi che potrebbero indurci a eseguire una verifica manuale del tuo account. Tali problemi includono, a titolo esemplificativo, quanto segue:

- I destinatari contattano SES per presentare un reclamo relativo alle e-mail inviate dal tuo account.
- Rileviamo delle modifiche insolite nei tuoi modelli di invio delle e-mail.
- I nostri filtri antispam individuano caratteristiche delle tue e-mail che sono tipiche dei contenuti non richiesti o di bassa qualità.

Quando mettiamo il tuo account in fase di verifica o sospendiamo la capacità del tuo account di inviare e-mail, ti inviamo una notifica. Nella maggior parte dei casi, questa notifica contiene informazioni sul problema e fornisce informazioni sulle misure successive che puoi adottare.

D3. Cosa sono le e-mail "indesiderate"?

Le e-mail indesiderate sono messaggi che il destinatario non ha chiesto esplicitamente di ricevere. Sono inclusi i casi in cui un destinatario si registra per un determinato tipo di e-mail, ad esempio le notifiche, e riceve invece un altro tipo di e-mail, ad esempio annunci pubblicitari.

Quando mettiamo il tuo account in fase di verifica o sospendiamo la capacità del tuo account di inviare e-mail, ti inviamo una notifica. Se ricevi una notifica che indica che stiamo intraprendendo una di queste azioni a causa di un problema con le e-mail indesiderate, accedi alla AWS Console e vai al Support Center. Rispondi al caso che abbiamo aperto per tuo conto. Nel tuo messaggio, includi le informazioni seguenti:

- Tutti i messaggi che invii sono espressamente richiesti dal destinatario e sono conformi alle policy di uso accettabile di AWS?

- Hai acquisito gli indirizzi e-mail in un modo diverso dall'interazione specifica di un cliente con te o il tuo sito Web o dalla richiesta del cliente di ricevere le e-mail? Devi descrivere come hai acquisito la tua lista mailing list.
- Come funzionano i tuoi processi di sottoscrizione e annullamento della sottoscrizione? Devi includere collegamenti per il consenso e il rifiuto espliciti.

D4. Cosa devo fare se ricevo una notifica indicante che il mio account è in fase di verifica o che l'invio è stato sospeso a causa di una verifica manuale?

Individua la causa del problema, quindi correggila. Dopo aver apportato modifiche che ritieni possano risolvere il problema, accedi alla AWS Console e vai al Support Center. Rispondi al caso che abbiamo aperto per tuo conto. Nel tuo messaggio, fornisci informazioni dettagliate sulle operazioni che hai effettuato per risolvere il problema e descrivi in che modo tali interventi potranno evitare che il problema si ripeta in futuro. Se riteniamo che le modifiche apportate possono risolvere in modo appropriato il problema, annulliamo il periodo di verifica del tuo account.

D5. Quali tipi di problemi considerate "risolvibili"?

In genere, riteniamo che la situazione sia risolvibile se hai uno storico di buone pratiche di invio e se esistono soluzioni che puoi adottare per eliminare il problema di invio continuando a inviare la maggior parte delle tue e-mail. Ad esempio, se invii tre tipi diversi di e-mail e solo uno è problematico, potresti voler semplicemente interrompere l'invio problematico e continuare con gli altri.

D6. Cosa succede se non riesco a individuare la causa del problema?

Puoi accedere alla AWS console e andare al Support Center. Rispondi alla pratica che abbiamo aperto per tuo conto e richiedi un esempio di messaggio che ha causato il problema.

Domande frequenti sulla DNS Blackhole List (DNSBL)

Le Domain Name System-based Blackhole Lists (DNSBL), a volte denominate Realtime Blackhole Lists (RBL), elenchi di mittenti bloccati, blocklist o blacklist, sono progettate per informare i provider di servizi di posta elettronica circa gli indirizzi IP sospettati dell'invio di e-mail indesiderate.

DNSBL differenti determinano conseguenze diverse in relazione alla capacità di recapitare e-mail. Questo argomento descrive come le DNSBL vanno a inficiare la distribuzione delle e-mail inviate utilizzando Amazon SES, nonché le nostre policy relative alla rimozione di indirizzi IP da tali elenchi.

> **Note**
>
> Questo argomento riguarda le DNSBL che i provider di posta elettronica utilizzano per bloccare i messaggi in entrata. Per informazioni sulle modalità con le quali Amazon SES blocca le e-mail in uscita inviate ai destinatari i cui indirizzi e-mail hanno generato in precedenza dei mancati recapiti, consulta Elenco di eliminazione globale Amazon SES.

D1. In che modo le DNSBL incidono sulla distribuzione di un messaggio e-mail?

Le diverse DNSBL incidono in modo diverso sulla corretta consegna di un messaggio. I principali provider di posta elettronica, tra cui Gmail, Hotmail e Yahoo, sembrano riconoscere come affidabili un numero decisamente ridotto di DNSBL, quali ad esempio quelle offerte da Spamhaus. In base alla nostra esperienza, gli altri elenchi tendono ad avere un impatto limitato, anche se alcuni sistemi di posta elettronica danno maggiore importanza ad alcune DNSBL piuttosto che ad altre.

Infine, molti provider di posta elettronica posseggono delle proprie liste di mittenti bloccati interne. I provider di posta elettronica proteggono questi elenchi in modo decisamente stretto e raramente li condividono con il pubblico. Se un indirizzo IP è presente su uno di questi elenchi, ciò può avere un maggiore impatto sulla capacità di inviare e-mail ai destinatari che utilizzano tale provider.

D2. In che modo gli indirizzi IP finiscono nelle DNSBL?

Un indirizzo IP può finire in una DNSBL in diversi modi. Gli indirizzi IP possono essere aggiunti a tali liste quando essi inviano e-mail a una trappola per spam. Una trappola per spam (o spamtrap) consiste in un indirizzo e-mail che non appartiene a un utente umano. Le spamtrap esistono al solo scopo raccogliere spam e identificare spammer. Alcune DNSBL, inoltre, consentono ai singoli utenti di inviare indirizzi IP. Alcune di tali liste consentono addirittura agli utenti di inviare interi intervalli di indirizzi IP. altre vengono gestite tramite contributi da parte degli amministratori delle e-mail e possono includere indirizzi IP che secondo gli amministratori utilizzano in modo improprio i loro sistemi.

D3. In che modo Amazon SES evita che i propri indirizzi IP compaiano nelle DNSBL?

I nostri sistemi ricercano dei segnali relativi a un uso illecito. Se rileviamo modelli o altre caratteristiche di invio che potrebbero determinare l'inserimento di un indirizzo IP in una DNSBL,

inviamo una notifica al mittente. Se la situazione è grave o se il mittente non è in grado di risolvere il problema dopo che abbiamo inviato la notifica, sospenderemo la possibilità di inviare e-mail finché il problema non viene risolto. Il rispetto della nostra policy di invio consente così di ridurre la possibilità che i nostri indirizzi IP vengano inseriti in DNSBL.

D4. È possibile per Amazon SES rimuovere gli indirizzi IP da una DNSBL?

Controlliamo attivamente le DNSBL che possono pregiudicare la consegna nell'ambito dell'intero servizio Amazon SES, o che possono incidere sulla possibilità di inviare e-mail ai destinatari che utilizzano i principali provider di posta elettronica, ad esempio Gmail, Yahoo, AOL e Hotmail. Le DNSBL offerte da Spamhaus rientrano in questa categoria. Quando uno dei nostri indirizzi IP appare su un elenco che soddisfa uno di questi criteri, interveniamo immediatamente affinché quell'indirizzo sia rimosso dalla DNSBL il più rapidamente possibile.

Non controlliamo invece le liste che solo difficilmente possono avere un qualche impatto sulla consegna nell'ambito dell'intero servizio di Amazon SES o che non presentano un impatto misurabile sul recapito ai principali provider di posta elettronica. Le DNSBL offerte da SORBS e UCEPROTECT rientrano in questa categoria. A causa delle specifiche procedure di pubblicazione e cancellazione delle offerte dei fornitori che gestiscono questi elenchi, non siamo in grado di rimuovere i nostri indirizzi IP da questi elenchi.

D5. Un provider di posta elettronica sta rifiutando le mie e-mail perché l'indirizzo IP di invio è presente in una DNSBL diversa da Spamhaus. Cosa posso fare?

In primo luogo, verifica che il messaggio è stato veramente bloccato a causa di un IP in DNSBL. Se la tua e-mail è stata rifiutata perché l'indirizzo IP di invio è stato inserito in DNSBL, riceverai una notifica di mancato recapito indicante il nome del provider dell'elenco, come nell'esempio seguente:

```
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
```

Se hai ricevuto una notifica di mancato recapito ma essa non contiene informazioni simili a quelle presenti nel messaggio indicato nell'esempio precedente, è più probabile che il provider di posta elettronica abbia respinto il messaggio per un motivo non correlato alla DNSBL.

Se sei in grado di confermare che un provider di posta elettronica sta bloccando la tua e-mail in quanto l'indirizzo IP di invio è presente su una DNSBL, puoi eseguire alcune operazioni:

- Contatta il postmaster del dominio che ha respinto il tuo messaggio per richiedere un'eccezione alla loro policy relativa ai filtri antispam. Alcuni postmaster possiedono dei processi di supporto e possono pubblicare una pagina postmaster che descrive il processo. Se il dominio che stai tentando di contattare non pubblica le sue policy relative al supporto postmaster, potresti contattare il postmaster mediante l'invio di e-mail all'indirizzo postmaster@*esempio.com*, dove *esempio.com* è il dominio in questione. In base allo standard RFC 5321 i domini devono avere una casella postmaster.

  Quando contatti il postmaster, devi fornire i codici di mancato recapito che hai ricevuto, le intestazioni delle e-mail che stai tentando di inviare, una misurazione dell'impatto che la DNSBL sta avendo sulla consegna delle tue e-mail nonché informazioni sulle ragioni per le quali ritieni che la tua e-mail sia stata bloccata in modo improprio. Maggiori sono le informazioni che puoi fornire al postmaster per dimostrare che stai inviando delle e-mail regolari, maggiori sono le probabilità che il postmaster faccia un'eccezione in tuo favore.
- Se il provider di posta elettronica non risponde o non è disposto a modificare le sue policy, ti consigliamo di utilizzare un indirizzo IP dedicato. Gli indirizzi IP dedicati sono indirizzi che puoi utilizzare soltanto tu. Implementando delle buone prassi di invio, puoi mantenere elevato il tuo tasso di coinvolgimento, mentre il tuo tasso di mancato recapito, reclamo e spamtrap può essere contenuto entro valori minimi. Delle buone prassi di invio possono aiutarti a evitare che i tuoi indirizzi siano inseriti nelle DNSBL.

D6. Le e-mail che invio a Gmail, Yahoo, Hotmail o a un altro dei principali provider vengono inviate alla cartella spam. Questo avviene perché il mio indirizzo IP di invio è presente su una DNSBL?

Probabilmente no. Se un indirizzo IP è presente in una DNSBL avente un impatto significativo, ad esempio una delle liste di Spamhaus, i principali provider di posta elettronica rifiuteranno completamente i messaggi da tale indirizzo IP, anziché inviarli alla cartella spam.

Quando i principali provider di posta elettronica accettano un'e-mail (invece di rifiutarla), essi in genere considerano il coinvolgimento dell'utente per determinare se posizionare il messaggio nella cartella della posta in arrivo o nella cartella spam. Il coinvolgimento dell'utente si riferisce ai modi in cui l'utente ha interagito con i messaggi inviati in precedenza.

Per incrementare le probabilità che i tuoi messaggi raggiungano la cartella della posta in arrivo dei clienti, ti consigliamo di implementare tutte le seguenti buone prassi:

- Non noleggiare o prendere a prestito elenchi di indirizzi e-mail. La locazione o l'acquisto di elenchi costituisce una violazione della Policy di utilizzo di AWS (AUP) e non è in alcun modo consentito in Amazon SES.
- Invia e-mail solo ai clienti che hanno esplicitamente richiesto di ricevere e-mail da parte tua. In molti paesi e giurisdizioni a livello mondiale, è illegale inviare e-mail a destinatari che non hanno esplicitamente accettato di riceverle.
- Interrompi l'invio di e-mail per i clienti che non hanno aperto o cliccato sui link presenti nei messaggi che hai inviato negli ultimi 30-90 giorni. Questo passaggio può aiutare a mantenere alti i tassi di coinvolgimento, aumentando così le probabilità che i messaggi inviati in futuro arrivino nelle caselle di posta dei destinatari.
- Utilizza elementi di progettazione consistenti e scrivi ogni messaggio da inviare adottando degli stili che consentano ai clienti di identificare facilmente i messaggi provenienti da te.
- Utilizza meccanismi di autenticazione delle e-mail, ad esempio SPF e DKIM.
- Quando i clienti utilizzano un modulo Web per ricevere le notifiche relative ai tuoi contenuti, invia loro un'e-mail che confermi il fatto che essi desiderano ricevere le tue e-mail. Non inviare ulteriori e-mail finché non confermano che desiderano ricevere e-mail da te. Questo processo è noto come consenso confermato o doppio consenso.
- Consenti ai tuoi clienti di annullare la sottoscrizione e rispetta immediatamente le richieste di annullamento della sottoscrizione.
- Se invii e-mail che contengono dei link, verifica tali link in relazione alla Domain Block List (DBL) di Spamhaus. Per verificare il funzionamento dei link, utilizza il Domain Lookup Tool presente sul sito Web Spamhaus.

Con l'implementazione di queste prassi, puoi migliorare la tua reputazione di mittente, il che contribuisce a mantenere elevata la probabilità che il messaggio e-mail inviato arrivi correttamente ai suoi destinatari. Inoltre, l'implementazione di queste pratiche aiuta mantenere basso il tasso di mancato recapito e reclamo per il tuo account, riducendo il rischio di invio di e-mail verso delle spamtrap.

Domande frequenti sui parametri per l'invio di e-mail con Amazon SES

Amazon SES raccoglie diversi parametri sulle e-mail che invii. Questi parametri ti consentono di analizzare l'efficacia del tuo programma di posta elettronica, nonché di monitorare le statistiche importanti, ad esempio le percentuali di mancato recapito e reclamo.

Questa sezione contiene le domande frequenti sui seguenti argomenti correlati ai parametri di invio di e-mail:

- Domande generali
- Monitoraggio delle aperture
- Monitoraggio dei clic

> **Note**
>
> Il monitoraggio degli eventi dipende dal provider di servizi di posta elettronica (ESP) del destinatario e da come ha configurato le impostazioni sulla privacy che sono al di fuori del controllo di Amazon SES. Il numero di eventi di tracciamento può essere distorto, restituendo conteggi imprecisi, in condizioni come:
>
> - Il destinatario dell'e-mail utilizza un provider di servizi di posta elettronica (ESP) che ne protegge la privacy.
> - Il destinatario dell'e-mail non concede esplicitamente al proprio ESP l'autorizzazione a condividere i propri dati.
> - L'ESP del destinatario dell'e-mail memorizza nella cache immagini o link; SES può conteggiare solo l'apertura iniziale, ma non sarà in grado di farlo con le aperture successive.

Domande generali

D1. Quando un'e-mail viene recapitata, per quanto tempo Amazon SES continua a raccogliere i parametri di apertura e di clic?

Amazon SES raccoglie i parametri di apertura e di clic per 60 giorni dopo l'invio di ogni e-mail.

D2. Se un utente apre un'e-mail più volte, o fa clic su un collegamento in un'e-mail più volte, ciascuno di tali eventi viene monitorato separatamente?

Se un destinatario apre un messaggio di posta elettronica più volte, Amazon SES conteggia ciascuna apertura come evento di apertura univoco. Analogamente, se un destinatario fa clic sullo stesso collegamento più volte, Amazon SES considera ogni clic come un evento di clic univoco. Tuttavia, questi conteggi possono essere distorti dagli scenari descritti sopra nella casella delle note.

D3. I parametri di apertura e di clic vengono aggregati oppure possono essere misurati fino al livello di destinatario?

Le aperture e i clic sono monitorati a livello di destinatario. Grazie a tale monitoraggio, puoi determinare quali destinatari hanno aperto un'e-mail o selezionato un collegamento all'interno di un'e-mail.

D4. Posso recuperare i parametri di apertura e di clic tramite l'API Amazon SES?

L'API Amazon SES non fornisce un metodo per il recupero dei parametri di apertura e di clic. Tuttavia, puoi recuperare tali parametri per Amazon SES tramite l'API CloudWatch. Ad esempio, puoi usare l'AWS CLI per recuperare i parametri di clic tramite l'API CloudWatch emettendo il comando seguente:

```
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
```

Il comando riportato in precedenza recupera il numero totale di eventi di clic per ogni giorno del 2017. Per recuperare i parametri di apertura, cambia il valore del parametro `metric-name` in `Open`. Puoi anche modificare i parametri `start-time` ed `end-time` per cambiare il periodo di analisi o il parametro `period` per un'analisi più dettagliata.

Monitoraggio delle aperture

D1. Come funziona il monitoraggio delle aperture?

In ogni e-mail inviata tramite Amazon SES è inserita un’immagine GIF trasparente di 1 pixel per 1 pixel e include un riferimento univoco a questo file immagine; quando l'immagine viene scaricata, Amazon SES è in grado di stabilire esattamente quale messaggio è stato aperto e da chi.

Di default, questo pixel viene inserito nella parte inferiore dell'e-mail; tuttavia, alcune applicazioni dei provider di posta elettronica troncano l'anteprima di un'e-mail quando supera una certa dimensione e potrebbero fornire un link per visualizzare il resto del messaggio. In questo scenario, l'immagine di tracciamento dei pixel SES non viene caricata ed eliminerà le percentuali di aperture che stai cercando di tracciare. Per aggirare questo problema, puoi opzionalmente posizionare il pixel all'inizio dell'e-mail o in qualsiasi altro luogo inserendo il segnaposto `{{ses:openTracker}}` nel corpo dell'e-mail. Una volta che SES riceve il messaggio con il segnaposto, verrà sostituito con l'immagine pixel di tracciamento aperta.

> **Important**
>
> Aggiungi un solo segnaposto `{{ses:openTracker}}`, poiché più di un segnaposto genererà la restituzione di un codice di errore `400 BadRequestException`.

L'aggiunta di questo pixel di monitoraggio non modifica l'aspetto della tua e-mail.

D2. Il monitoraggio delle aperture è abilitato per impostazione predefinita?

Il monitoraggio delle aperture è disponibile per tutti gli utenti di Amazon SES per impostazione predefinita. Per utilizzarlo, è necessario eseguire le operazioni seguenti:

1. Crea un set di configurazione.
2. Nel set di configurazione, crea una destinazione di evento.
3. Configura la destinazione di evento per pubblicare le notifiche di eventi di apertura in una destinazione.
4. In ogni e-mail per cui desideri monitorare le aperture, specifica il set di configurazione creato nella fase 1.

Per informazioni dettagliate su come abilitare il tracciamento aperto attraverso la destinazione degli eventi di un set di configurazione, vedere the section called “Crea destinazioni degli eventi”. È possibile utilizzare il segnaposto pixel in E-mail SMTP come e-mail formattata, raw e basata su modelli.

Ulteriori informazioni su come Monitoraggio dell'invio di e-mail utilizzando la pubblicazione di eventi.

D3. Posso omettere il pixel di monitoraggio delle aperture da determinate e-mail?

Sono disponibili due modi per omettere il pixel di monitoraggio dell'apertura dalle tue e-mail. Il primo metodo consiste nell'invio di e-mail senza specificare un set di configurazione. In alternativa, puoi specificare un set di configurazione che non sia configurato per pubblicare dati relativi a eventi di apertura.

D4. Monitori le aperture per e-mail non crittografate?

Il monitoraggio delle aperture funziona solo con e-mail HTML. Poiché il monitoraggio delle aperture si basa sull'inclusione di un'immagine, non è possibile raccogliere i parametri di apertura per gli utenti che aprono e-mail tramite un client e-mail di solo testo (non HTML).

Monitoraggio dei clic

D1. Come funziona il monitoraggio dei clic?

Per monitorare i clic, Amazon SES modifica ogni collegamento nel corpo dell'e-mail. Quando i destinatari aprono un collegamento, vengono indirizzati a un server Amazon SES, quindi immediatamente reinviati all'indirizzo di destinazione. Come per il monitoraggio delle aperture, ogni collegamento di reindirizzamento è univoco. In questo modo Amazon SES è in grado di determinare quale destinatario ha selezionato il collegamento, quando e da quale e-mail ha raggiunto il collegamento.

> **Important**
>
> Se invii un solo messaggio a più destinatari, ogni destinatario salverà lo stesso collegamento di monitoraggio dei clic. Per monitorare l'attività di selezione dei singoli destinatari, invia un'e-mail a un solo destinatario per operazione di invio.

D2. Posso disabilitare il monitoraggio dei clic?

Puoi disabilitare il monitoraggio dei singoli collegamenti aggiungendo un attributo, `ses:no-track`, ai tag di ancoraggio nel corpo HTML della tua e-mail. Ad esempio, se ti colleghi alla home page di AWS, un normale collegamento di ancoraggio assomiglia al seguente:

```
<a href="https://aws.amazon.com">Amazon Web Services</a>
```

Per disabilitare il rilevamento dei clic per quel collegamento, modificarlo in modo simile al seguente:

```
<a ses:no-track href="aws.amazon.com">Amazon Web Services</a>
```

Poiché `ses:no-track` non è un attributo HTML standard, Amazon SES lo rimuove automaticamente dalla versione dell'e-mail che arriva nella casella di posta in arrivo dei destinatari.

È inoltre possibile disabilitare il rilevamento dei clic per tutti i messaggi inviati utilizzando un set di configurazione specifico. Per disabilitare il rilevamento dei clic, modificare la destinazione dell'evento del set di configurazione in modo che non acquisisca gli eventi di clic.

Per informazioni dettagliate su come abilitare e disabilitare il monitoraggio dei clic attraverso la destinazione degli eventi di un set di configurazione, vederethe section called “Crea destinazioni degli eventi”.

Ulteriori informazioni su come Monitoraggio dell'invio di e-mail utilizzando la pubblicazione di eventi.

D3. Quanti link possono essere tracciati in ogni e-mail?

Il sistema di monitoraggio dei clic può monitorare un massimo di 250 link.

D4. I parametri di clic vengono raccolti per i collegamenti nelle e-mail non crittografate?

È possibile tenere traccia solo dei clic nelle e-mail HTML.

D5. Posso aggiungere tag ai collegamenti con identificatori univoci?

Puoi aggiungere un numero illimitato di tag, come coppie chiave-valore, ai collegamenti nella tua e-mail utilizzando l'attributo `ses:tags`. Quando usi questo attributo, specifica le chiavi e i valori con lo stesso formato che utilizzeresti per trasferire proprietà CSS in linea: digita la chiave, seguita da due punti (:), quindi dal valore. Se hai bisogno di trasferire diverse coppie chiave-valore, separa ciascuna con un punto e virgola (;).

Ad esempio, supponiamo che desideri aggiungere i tag `product:book, genre:fiction, subgenre:scifi, type:newrelease` a un collegamento. Il collegamento risultante è analogo al seguente:

```
<a ses:tags="product:book;genre:fiction;subgenre:scifi;type:newrelease;"
    href="http://www.amazon.com/…/">New Releases in Science Fiction</a>
```

Questi tag sono trasferiti attraverso la tua destinazione di pubblicazione degli eventi in modo che tu possa eseguire un'analisi aggiuntiva sui collegamenti specifici sui quali gli utenti hanno fatto clic.

> **Note**
>
> I tag di collegamento possono includere numeri da 0 a 9, lettere da A a Z (maiuscole e minuscole), trattini (-) e trattini di sottolineatura (_).

D6. I collegamenti monitorati utilizzano il protocollo HTTP o HTTPS?

I collegamenti di monitoraggio utilizzano lo stesso protocollo dei collegamenti originali nella tua e-mail.

Ad esempio, se la tua e-mail include un collegamento a `https://www.amazon.com`, questo viene sostituito con un collegamento di monitoraggio che utilizza il protocollo HTTPS. Se la tua e-mail include un collegamento a `http://www.example.com`, questo viene sostituito con un collegamento di monitoraggio che utilizza HTTP. Se la tua e-mail include entrambi i collegamenti menzionati in precedenza, il collegamento HTTPS viene sostituito con un collegamento di monitoraggio che utilizza il protocollo HTTPS e il collegamento HTTP viene sostituito con un collegamento di monitoraggio che utilizza il protocollo HTTP.

D7. Un collegamento in un'e-mail non viene monitorato. Perché?

Amazon SES si aspetta che i collegamenti nella tua e-mail contengano URL codificati correttamente. Nello specifico, gli URL nel tuo link devono rispettare lo standard RFC 3986. Se un collegamento in un'e-mail non è codificato correttamente, i destinatari continueranno a vedere il collegamento contenuto nel messaggio e-mail, ma Amazon SES non potrà tenere traccia degli eventi per quel collegamento.

Problemi correlati a errori di codifica in genere si verificano in URL che contengono stringhe di query. Ad esempio, se l'URL di un collegamento nella tua e-mail contiene un carattere di spaziatura non codificato nella stringa di query (ad esempio lo spazio tra "John" e "Doe" nell'esempio seguente: http://www.example.com/path/to/page?name=John Doe), Amazon SES non potrà monitorare tale collegamento. Tuttavia, se l'URL usa invece un carattere di spaziatura codificato (ad esempio "%20" nell'esempio seguente: http://www.example.com/path/to/page?name=John%20Doe), Amazon SES potrà monitorarlo correttamente.

Indice di ricerca rapida

Il seguente indice è stato creato per aiutarti a trovare rapidamente elementi in Amazon SES attraverso due modalità di ricerca: per istruzioni o per concetti. Le istruzioni descrivono le procedure mentre i concetti spiegano il quadro generale.

Facci sapere cosa ne pensi

Utilizza il pulsante Feedback nell'angolo in alto a destra per farci sapere...

- Questo indice è stato utile?
- Ci sono istruzioni o concetti che vorresti che siano aggiunti a questo indice?
- Pensi ci sia qualcosa che avrebbe dovuto essere classificato in modo diverso?

Link ai concetti e alle istruzioni SES

How-tos

I link alle istruzioni SES sono elencati in ordine alfabetico e ti porteranno alla sezione corrispondente in cui viene descritta la procedura per eseguire l'azione selezionata.

- Scopri come…
  - Aggiungere un record SPF come parte della configurazione di un dominio MAIL FROM personalizzato
  - Assegnare pool di indirizzi IP
  - Blocco dello SPAM per la ricezione di e-mail
  - Configurare domini personalizzati di apertura e clic
  - Configurare le notifiche SNS
  - Connettersi a un endpoint SMTP
  - Creare un set di configurazione
  - Creare un'identità del dominio
  - Creare un'identità dell'indirizzo e-mail
  - Creare destinazioni degli eventi
  - Creare filtri degli indirizzi IP

- Creazione di un pool di IP gestiti per abilitare gli IP dedicati (gestiti)
- Creare regole di ricezione
- Creare allarmi di reputazione tramite CloudWatch
- Creare una policy per l'autorizzazione all'invio tramite una policy personalizzata
- Creare una policy di autorizzazione di invio tramite il generatore di policy
- Creazione di pool di IP dedicati standard per indirizzi IP dedicati (standard)
- Eliminare un'identità
- Eliminare dati personali
- Modificare di un'identità
- Abilitare l'inoltro del feedback e-mail
- Esportare i parametri di reputazione
- Uscire dal sandbox
- Nozioni di base su SES
- Iniziare a utilizzare Virtual Deliverability Manager
- Assegnare le autorizzazioni per la ricezione di e-mail
- Aumentare il throughput
- Aumentare le quote di invio
- Integrare con il server di posta esistente
- Registrare le chiamate API
- Gestire un set di configurazione
- Gestire Easy DKIM e BYODKIM
- Monitorare i parametri di invio e reputazione
- Monitorare le statistiche di invio
- Monitorare le statistiche di utilizzo
- Monitorare la quota di invio
- Ottenere i registri DKIM per un'identità
- Ottenere le credenziali SMTP
- Sostituire l'eliminazione a livello di account con l'eliminazione a livello di set di configurazione
- Sovrascrivere la firma DKIM ereditata su un'identità di indirizzo e-mail
- Sospendere l'invio di e-mail

- Pubblicare un registro MX
- Segnalare un utilizzo illecito delle risorse AWS
- Richiedere indirizzi IP dedicati
- Richiedere supporto tecnico
- Risolvi i problemi di efficacia del recapito e di reputazione grazie all'advisor di Virtual Deliverability Manager
- Recuperare dati di eventi da CloudWatch
- Recuperare dati di eventi da Kinesis Data Firehose
- Recuperare dati di eventi da SNS
- Inviare un'e-mail tramite un SDK AWS
- Inviare e-mail a livello di programmazione
- Inviare e-mail tramite l'API SES
- Inviare e-mail tramite SMTP
- Inviare e-mail non formattate con un allegato utilizzando la CLI o l'API SES
- Inviare e-mail di prova utilizzando il simulatore di cassette postali
- Configurare BYODKIM (Utilizza il tuo DKIM)
- Configurare una policy DMARC
- Configurare Easy DKIM
- Configurare la ricezione di e-mail
- Configurare la pubblicazione di eventi
- Configurare un dominio MAIL FROM
- Configurare l'autorizzazione di invio (attività del proprietario di identità)
- Configurare l'autorizzazione di invio (attività del mittente delegato)
- Specificare un set di configurazione per l'invio di e-mail
- Verificare la connessione all'interfaccia SMTP
- Tenere traccia della frequenza di mancati recapiti e reclami
- Scoprire le proprietà della firma DKIM ereditate
- Utilizzare parametri di reputazione
- Utilizzare pacchetti software per l'invio di e-mail
- Utilizzare la gestione delle sottoscrizioni

- Utilizzare i modelli per l'invio di e-mail
- Utilizzare l'elenco di eliminazioni a livello di account
- Verificare un'identità di dominio
- Verificare l'identità di un indirizzo e-mail
- Visualizzare un'identità
- Visualizzare a livello generale e in dettaglio i parametri di efficacia del recapito per il tuo account grazie alla dashboard di Virtual Deliverability Manager
- Visualizzare i parametri SNDS per gli indirizzi IP dedicati
- Preparare gli indirizzi IP dedicati

Concepts

I link ai concetti di SES sono elencati in ordine alfabetico e ti porteranno al capitolo e alle sezioni corrispondenti in cui viene spiegato il concetto selezionato.

- Trova informazioni su...
  - Segnalazione di utilizzo illecito di risorse AWS
  - Pannello di controllo dell'account
  - Elenco di eliminazione a livello di account
  - Opzioni di azione per la ricezione di e-mail
  - Operazione di aggiunta intestazioni
  - Tipi di allegati, non supportati
  - Operazione di risposta mancato recapito, ritorno
  - BYODKIM (Utilizza il tuo DKIM)
  - BYOIP(Utilizza il tuo IP)
  - Esempi di codice
  - Convalida della conformità
  - Eliminazione a livello di set di configurazione
  - Set di configurazione
  - Codifiche dei contenuti
  - Supporto legacy delle notifiche tra account
  - Dominio MAIL FROM personalizzato

- Protezione dei dati
- Indirizzi IP dedicati
- Indirizzi IP dedicati (gestiti)
- Indirizzi IP dedicati (standard)
- DKIM, autenticazione delle e-mail con
- DMARC(Verifica, segnalazione e conformità dei messaggi in base al dominio)
- DMARC tramite DKIM, conformità
- DMARC tramite SPF, conformità
- Easy DKIM
- Destinazione dell'inoltro di feedback via e-mail
- Autenticazione della ricezione e-mail
- Concetti relativi alla ricezione di e-mail
- Spiegazioni passo per passo della console di ricezione e-mail
- Scansione del malware di ricezione e-mail
- Autorizzazioni di ricezione e-mail
- Casi d'uso di ricezione e-mail
- Restrizioni per la ricezione e-mail
- Metodi di autenticazione per l'invio di e-mail
- Endpoint
- Notifiche eventi
- Notifiche di eventi tramite e-mail
- Notifiche di eventi tramite SNS
- Event publishing (Pubblicazione degli eventi)
- Domande frequenti
- Elenco di eliminazione globale
- Campi di intestazione supportati
- Identità, gestione
- Identity and Access Management
- Sicurezza dell'infrastruttura

- Operazione di integrazione con Amazon WorkMail

- Controllo basato su IP mediante filtri di indirizzi IP
- Operazione della funzione Lambda, chiamata
- Gestione elenchi
- Elenchi e abbonamenti
- Registrazione e monitoraggio
- Rilevamento di malware
- Firma DKIM manuale
- Monitoraggio dell'invio di e-mail utilizzando la pubblicazione di eventi
- Monitoraggio della reputazione del mittente
- Monitoraggio dell'attività di invio
- Quote
- Regole di ricezione
- Controllo basato sul destinatario mediante regole di ricezione
- Regioni
- Parametri di reputazione
- Messaggi sui parametri di reputazione
- Resilienza
- Operazione del bucket S3, consegna
- Sandbox: uscita
- Sicurezza
- Protocolli di sicurezza supportati
- Autorizzazione di invio
- Invio dell'anatomia della policy di autorizzazione
- Esempi di policy di autorizzazione di invio
- Processo di autorizzazione di invio
- Parametri SNDS per gli indirizzi IP dedicati
- Contenuti delle notifiche SNS
- Esempi di notifiche SNS
- Azione di un argomento SNS: pubblicazione

- SPF (Sender Policy Framework)

- Operazione di interruzione del set di regole
- Gestione delle sottoscrizioni
- Richiesta di supporto tecnico
- Modelli per la verifica di e-mail personalizzate
- Risoluzione dei problemi
- Identità verificate
- Virtual Deliverability Manager
- Endpoint VPC

Le traduzioni sono generate tramite traduzione automatica. In caso di conflitto tra il contenuto di una traduzione e la versione originale in Inglese, quest'ultima prevarrà.