Benutzerhandbuch

AWS Social Messaging für Endbenutzer

AWS Social Messaging für Endbenutzer: Benutzerhandbuch

Table of Contents

Was ist AWS End User Messaging Social?

AWS End User Messaging Social, auch Social Messaging genannt, ist ein Messaging-Dienst, der es Entwicklern ermöglicht, ihn WhatsApp in ihre Anwendungen zu integrieren. Er bietet Zugriff auf die WhatsApp Messaging-Funktionen und ermöglicht die Erstellung von markenspezifischen, interaktiven Inhalten mit Bildern, Videos und Schaltflächen. Mithilfe dieses Dienstes können Sie Ihren Anwendungen neben bestehenden Kanälen wie SMS und Push-Benachrichtigungen auch WhatsApp Messaging-Funktionen hinzufügen. Auf diese Weise können Sie mit Kunden über ihren bevorzugten Kommunikationskanal in Kontakt treten.

Erstellen Sie zunächst entweder mithilfe des selbstgesteuerten Onboarding-Prozesses in der AWS End User Messaging Social-Konsole ein neues WhatsApp Geschäftskonto (WABA) oder verknüpfen Sie ein vorhandenes WABA mit dem Service.

Themen

Verwenden Sie AWS End User Messaging Social zum ersten Mal?

Wenn Sie AWS End User Messaging Social zum ersten Mal verwenden, empfehlen wir Ihnen, zunächst die folgenden Abschnitte zu lesen:

- AWS Endanwender-Messaging Social einrichten
- Erste Schritte mit AWS End User Messaging Social
- Bewährte Methoden für Social Messaging für AWS Endbenutzer

Funktionen von AWS End User Messaging Social

AWS End User Messaging Social bietet die folgenden Funktionen und Fähigkeiten:

- Entwerfen Sie konsistente Nachrichten und verwenden Sie Inhalte effektiver wieder, indem Sie Nachrichtenvorlagen erstellen und verwenden. Eine Nachrichtenvorlage enthält Inhalte und Einstellungen, die Sie in von Ihnen gesendeten Nachrichten wiederverwenden möchten.
- Zugriff auf umfangreiche Messaging-Funktionen für ein ansprechenderes Erlebnis. Neben Text und Medien können Sie auch Standorte und interaktive Nachrichten senden.
- Empfangen Sie eingehende Text- und Mediennachrichten von Ihren Kunden.
- Bauen Sie Vertrauen bei Ihren Kunden auf, indem Sie Ihre Geschäftsidentität über Meta verifizieren.

Zugehörige Services

AWS bietet weitere Messaging-Dienste an, die zusammen in einem Mehrkanal-Workflow verwendet werden können:

- Verwenden Sie AWS End User Messaging SMS, um SMS-Nachrichten zu senden
- Verwenden Sie AWS End User Messaging Push, um Push-Benachrichtigungen zu senden
- Verwenden Sie Amazon SES, um E-Mails zu senden

Zugreifen auf AWS End User Messaging Social

Sie können wie folgt auf AWS End User Messaging Social zugreifen:

AWS Konsole für Endbenutzer-Messaging Social

Die Weboberfläche, auf der Sie Ressourcen erstellen und verwalten.

AWS Command Line Interface

Interagieren AWS-Services Sie mithilfe von Befehlen in Ihrer Befehlszeilen-Shell. Das AWS Command Line Interface wird unter Windows, MacOS und Linux unterstützt. Weitere Informationen zu finden Sie im AWS CLIAWS Command Line Interface Benutzerhandbuch. Die Befehle für AWS End User Messaging Social finden Sie in der AWS CLI Befehlsreferenz.

AWS SDKs

Wenn Sie es vorziehen, Anwendungen sprachspezifisch zu erstellen, APIs anstatt eine Anfrage über HTTP oder HTTPS einzureichen, verwenden Sie die Bibliotheken, den Beispielcode, die

Tutorials und andere Ressourcen von. AWS Diese Bibliotheken bieten grundlegende Funktionen zur Automatisierung von Aufgaben, wie z. B. das kryptografische Signieren Ihrer Anfragen, das Wiederholen von Anfragen und das Behandeln von Fehlerantworten. Diese Funktionen erleichtern Ihnen den Einstieg. Weitere Informationen finden Sie unter Tools, auf denen Sie aufbauen können AWS.

Regionale Verfügbarkeit

AWS End User Messaging Social ist in mehreren Ländern AWS-Regionen in Nordamerika, Europa, Asien und Ozeanien verfügbar. AWS Unterhält in jeder Region mehrere Availability Zones. Diese Availability Zones sind physisch voneinander isoliert, jedoch durch private, hochredundante Netzwerkverbindungen mit geringer Latenz und hohem Durchsatz miteinander verbunden. Diese Availability Zones werden verwendet, um ein hohes Maß an Verfügbarkeit und Redundanz zu gewährleisten und gleichzeitig die Latenz zu minimieren.

Weitere Informationen dazu finden Sie unter Geben Sie an AWS-Regionen, was AWS-Regionen Ihr Konto verwenden kann in der. Allgemeine Amazon Web Services-Referenz Eine Liste aller Regionen, in denen AWS End User Messaging Social derzeit verfügbar ist, sowie die Endpunkte für jede Region finden Sie unter Endpunkte und Kontingente für AWS End User Messaging Social API und AWS Dienstendpunkte in der Allgemeine Amazon Web Services-Referenzoder der folgenden Tabelle. Weitere Informationen über die in jeder Region verfügbare Anzahl von Availability Zones finden Sie unter Globale AWS -Infrastruktur.

Verfügbarkeit in Regionen

Name der Region	Region	Endpunkt	WhatsApp API-Version
USA Ost (Nord-Virginia)	us-east-1	social-messaging.us-east-1.amazonaws.com social-messaging.us-east-1.api.aws social-messaging-fips.us-east-1.amazonaws.com	Version 20 und höher

Name der Region	Region	Endpunkt	WhatsApp API-Version
		social-messaging-fips.us-east-1.api.aws	
USA Ost (Ohio)	us-east-2	social-messaging.us-east-2.amazonaws.com social-messaging.us-east-2.api.aws social-messaging-fips.us-east-2.amazonaws.com social-messaging-fips.us-east-2.api.aws	Version 20 und höher
USA West (Oregon)	us-west-2	social-messaging.us-west-2.amazonaws.com social-messaging.us-west-2.api.aws social-messaging-fips.us-west-2.amazonaws.com social-messaging-fips.us-west-2.api.aws	Version 20 und höher

Name der Region	Region	Endpunkt	WhatsApp API-Version
Kanada (Zentral)	ca-central-1	social-messaging.ca-central-1.amazonaws.com social-messaging.ca-central-1.api.aws social-messaging-fips.ca-central-1.amazonaws.com social-messaging-fips.ca-central-1.api.aws	Version 20 und höher
Afrika (Kapstadt)	af-south-1	social-messaging.af-south-1.amazonaws.com social-messaging.af-south-1.api.aws	Version 20 und höher
Asien-Pazifik (Tokio)	ap-northeast-1	social-messaging.ap-northeast-1.amazonaws.com social-messaging.ap-northeast-1.api.aws	Version 20 und höher
Asien-Pazifik (Seoul)	ap-northeast-2	social-messaging.ap-northeast-2.amazonaws.com social-messaging.ap-northeast-2.api.aws	Version 20 und höher

Name der Region	Region	Endpunkt	WhatsApp API-Version
Asien-Pazifik (Mumbai)	ap-south-1	social-messaging.ap-south-1.amazonaws.com social-messaging.ap-south-1.api.aws	Version 20 und höher
Asien-Pazifik (Hyderabad)	ap-south-2	social-messaging.ap-south-2.amazonaws.com social-messaging.ap-south-2.api.aws	Version 20 und höher
Asien-Pazifik (Singapur)	ap-southeast-1	social-messaging.ap-southeast-1.amazonaws.com social-messaging.ap-southeast-1.api.aws	Version 20 und höher
Asien-Pazifik (Sydney)	ap-southeast-2	social-messaging.ap-southeast-2.amazonaws.com social-messaging.ap-southeast-2.api.aws	Version 20 und höher
Europa (Frankfurt)	eu-central-1	social-messaging.eu-central-1.amazonaws.com social-messaging.eu-central-1.api.aws	Version 20 und höher

Name der Region	Region	Endpunkt	WhatsApp API-Version
Europa (Spanien)	eu-south-2	social-messaging.eu-south-2.amazonaws.com social-messaging.eu-south-2.api.aws	Version 20 und höher
Europa (Irland)	eu-west-1	social-messaging.eu-west-1.amazonaws.com social-messaging.eu-west-1.api.aws	Version 20 und höher
Europa (London)	eu-west-2	social-messaging.eu-west-2.amazonaws.com social-messaging.eu-west-2.api.aws	Version 20 und höher
Südamerika (São Paulo)	sa-east-1	social-messaging.sa-east-1.amazonaws.com social-messaging.sa-east-1.api.aws	Version 20 und höher

AWS Endanwender-Messaging Social einrichten

Bevor Sie AWS End User Messaging Social zum ersten Mal verwenden können, müssen Sie die folgenden Schritte ausführen.

Themen

Melden Sie sich an für ein AWS-Konto

Wenn Sie noch keine haben AWS-Konto, führen Sie die folgenden Schritte aus, um eine zu erstellen.

Um sich für eine anzumelden AWS-Konto

1. Öffnen Sie https://portal.aws.amazon.com/billing/die Anmeldung.
2. Folgen Sie den Online-Anweisungen.

   Ein Teil des Anmeldevorgangs umfasst den Empfang eines Telefonanrufs oder einer Textnachricht und die Eingabe eines Bestätigungscodes auf der Telefontastatur.

   Wenn Sie sich für eine anmelden AWS-Konto, wird eine Root-Benutzer des AWS-Kontoserstellt. Der Root-Benutzer hat Zugriff auf alle AWS-Services und Ressourcen des Kontos. Als bewährte Sicherheitsmethode weisen Sie einem Administratorbenutzer Administratorzugriff zu und verwenden Sie nur den Root-Benutzer, um Aufgaben auszuführen, die Root-Benutzerzugriff erfordern.

AWS sendet Ihnen nach Abschluss des Anmeldevorgangs eine Bestätigungs-E-Mail. Du kannst jederzeit deine aktuellen Kontoaktivitäten einsehen und dein Konto verwalten, indem du zu https://aws.amazon.com/gehst und Mein Konto auswählst.

Erstellen eines Benutzers mit Administratorzugriff

Nachdem Sie sich für einen angemeldet haben AWS-Konto, sichern Sie Ihren Root-Benutzer des AWS-Kontos AWS IAM Identity Center, aktivieren und erstellen Sie einen Administratorbenutzer, sodass Sie den Root-Benutzer nicht für alltägliche Aufgaben verwenden.

Sichern Sie Ihre Root-Benutzer des AWS-Kontos

1. Melden Sie sich AWS Management Consoleals Kontoinhaber an, indem Sie Root-Benutzer auswählen und Ihre AWS-Konto E-Mail-Adresse eingeben. Geben Sie auf der nächsten Seite Ihr Passwort ein.

   Hilfe bei der Anmeldung mit dem Root-Benutzer finden Sie unter Anmelden als Root-Benutzer im AWS-Anmeldung Benutzerhandbuch zu.

2. Aktivieren Sie die Multi-Faktor-Authentifizierung (MFA) für den Root-Benutzer.

   Anweisungen finden Sie unter Aktivieren eines virtuellen MFA-Geräts für Ihren AWS-Konto Root-Benutzer (Konsole) im IAM-Benutzerhandbuch.

Erstellen eines Benutzers mit Administratorzugriff

1. Aktivieren Sie das IAM Identity Center.

   Anweisungen finden Sie unter Aktivieren AWS IAM Identity Center im AWS IAM Identity Center Benutzerhandbuch.

2. Gewähren Sie einem Administratorbenutzer im IAM Identity Center Benutzerzugriff.

   Ein Tutorial zur Verwendung von IAM-Identity-Center-Verzeichnis als Identitätsquelle finden Sie IAM-Identity-Center-Verzeichnis im Benutzerhandbuch unter Benutzerzugriff mit der Standardeinstellung konfigurieren.AWS IAM Identity Center

Anmelden als Administratorbenutzer

- Um sich mit Ihrem IAM-Identity-Center-Benutzer anzumelden, verwenden Sie die Anmelde-URL, die an Ihre E-Mail-Adresse gesendet wurde, als Sie den IAM-Identity-Center-Benutzer erstellt haben.

Hilfe bei der Anmeldung mit einem IAM Identity Center-Benutzer finden Sie im AWS-Anmeldung Benutzerhandbuch unter Anmeldung beim AWS Access-Portal.

Weiteren Benutzern Zugriff zuweisen

1. Erstellen Sie im IAM-Identity-Center einen Berechtigungssatz, der den bewährten Vorgehensweisen für die Anwendung von geringsten Berechtigungen folgt.

   Anweisungen hierzu finden Sie unter Berechtigungssatz erstellen im AWS IAM Identity Center Benutzerhandbuch.
2. Weisen Sie Benutzer einer Gruppe zu und weisen Sie der Gruppe dann Single Sign-On-Zugriff zu.

   Eine genaue Anleitung finden Sie unter Gruppen hinzufügen im AWS IAM Identity Center Benutzerhandbuch.

Nächste Schritte

Nun, da Sie bereit sind, mit AWS End User Messaging Social zu arbeiten, finden Sie weitere Informationen Erste Schritte mit AWS End User Messaging Social zur Erstellung Ihres WhatsApp Geschäftskontos (WABA) oder zur Migration Ihres bestehenden WhatsApp Geschäftskontos.

Erste Schritte mit AWS End User Messaging Social

Diese Themen führen Sie durch die Schritte, um Ihr WhatsApp Geschäftskonto (WABA) mit AWS End User Messaging Social zu verknüpfen oder zu migrieren.

Themen

Melden Sie sich an für WhatsApp

Ein WhatsApp Geschäftskonto (WABA) ermöglicht es Ihrem Unternehmen, die WhatsApp Geschäftsplattform zu nutzen, um Nachrichten direkt an Ihre Kunden zu senden. Sie alle WABAs sind Teil Ihres Meta-Geschäftsportfolios. Eine WABA enthält Ihre kundenorientierten Ressourcen wie Telefonnummer, Vorlagen und WhatsApp Geschäftsprofil. Ein WhatsApp Unternehmensprofil enthält die Kontaktinformationen Ihres Unternehmens, die Benutzer sehen können. Weitere Informationen zu WhatsApp Geschäftskonten finden Sie unterWhatsApp Geschäftskonto (WABA) in AWS End User Messaging Social.

Folgen Sie den Schritten in diesem Abschnitt, um mit AWS End User Messaging Social zu beginnen. Verwenden Sie den eingebetteten Anmeldeprozess, um entweder ein neues WhatsApp Geschäftskonto (WABA) zu erstellen oder ein vorhandenes WABA zu AWS End User Messaging Social zu migrieren.

Voraussetzungen

Important

Mit Meta/ arbeiten WhatsApp

- Ihre Nutzung der WhatsApp Business Solution unterliegt den Bedingungen der Nutzungsbedingungen für Unternehmen, den Nutzungsbedingungen für WhatsApp Business Solution, der WhatsApp Business Messaging-Richtlinie, den WhatsApp Messaging-Richtlinien und allen anderen Bestimmungen, Richtlinien oder Richtlinien, die durch Bezugnahme darin enthalten sind (die jeweils von Zeit zu Zeit aktualisiert werden können). WhatsApp

- Meta oder WhatsApp kann Ihnen jederzeit die Nutzung der WhatsApp Business Solution verbieten.
- Sie müssen ein WhatsApp Geschäftskonto („WABA“) bei Meta und einrichten. WhatsApp
- Sie müssen ein Business Manager-Konto bei Meta erstellen und es mit Ihrer WABA verknüpfen.
- Sie müssen uns die Kontrolle über Ihre WABA geben. Auf Ihren Wunsch hin übertragen wir Ihnen die Kontrolle über Ihre WABA in angemessener und zeitnaher Weise zurück und verwenden dabei die Methoden, die Meta uns zur Verfügung stellt.
- Im Zusammenhang mit Ihrer Nutzung der WhatsApp Business Solution werden Sie keine Inhalte, Informationen oder Daten übermitteln, die Schutzvorschriften unterliegen. and/or limitations on distribution pursuant to applicable laws and/or
- WhatsAppDie Preise für die Nutzung der WhatsApp Business Solution finden Sie unter Conversation-Based Pricing.

- Um ein WhatsApp Geschäftskonto (WABA) zu erstellen, benötigt Ihr Unternehmen ein Meta-Geschäftskonto. Prüfen Sie, ob Ihr Unternehmen bereits über ein Meta-Geschäftskonto verfügt. Wenn Sie kein Meta-Geschäftskonto haben, können Sie während des Anmeldevorgangs eines erstellen.
- Um eine Telefonnummer zu verwenden, die bereits mit der WhatsApp Messenger-Anwendung oder der WhatsApp Business-Anwendung verwendet wird, müssen Sie sie zuerst löschen.
- Eine Telefonnummer, die entweder eine SMS oder einen Einmalpasscode (OTP) per Spracheingabe empfangen kann. Die für die Registrierung verwendete Telefonnummer wird mit Ihrem WhatsApp Konto verknüpft, und die Telefonnummer wird verwendet, wenn Sie Nachrichten senden. Die Telefonnummer kann weiterhin für SMS, MMS und Sprachnachrichten verwendet werden.
- Wenn Sie eine bestehende WABA importieren, benötigen Sie die PINs für alle Telefonnummern, die mit der importierten WABA verknüpft sind. Um eine verlorene oder vergessene PIN zurückzusetzen, folgen Sie den Anweisungen unter PIN aktualisieren in der WhatsApp Business Platform Cloud API-Referenz.

Die folgenden Voraussetzungen müssen erfüllt sein, um entweder ein Amazon SNS SNS-Thema oder eine Amazon Connect Connect-Instance als Nachrichten- und Ereignisziel verwenden zu können.

Amazon SNS-Thema

- Ein Amazon SNS SNS-Thema wurde erstellt und Berechtigungen wurden hinzugefügt.

> **Note**
>
> Amazon-SNS-FIFO-Themen werden nicht unterstützt.

- (Optional) Um ein Amazon SNS SNS-Thema zu verwenden, das mit AWS KMS Schlüsseln verschlüsselt ist, müssen Sie AWS End User Messaging Social-Berechtigungen für die bestehende Schlüsselrichtlinie gewähren.

Amazon Connect Connect-Instanz

- Eine Amazon Connect Connect-Instanz wurde erstellt und Berechtigungen wurden hinzugefügt.

Melden Sie sich über die Konsole an

Folgen Sie diesen Anweisungen, um ein neues WhatsApp Konto zu erstellen, Ihr bestehendes Konto zu migrieren oder einer bestehenden WABA eine Telefonnummer hinzuzufügen. Im Rahmen des Anmeldevorgangs gewähren Sie AWS End User Messaging Social Zugriff auf Ihr WhatsApp Geschäftskonto. Außerdem gestatten Sie AWS End User Messaging Social, Ihnen Nachrichten in Rechnung zu stellen. Weitere Informationen zu WhatsApp Geschäftskonten finden Sie unterGrundlegendes WhatsApp zu Geschäftskontotypen.

1. Öffnen Sie die AWS End User Messaging Social-Konsole unter https://console.aws.amazon.com/social-messaging/.
2. Wählen Sie Geschäftskonten aus.
3. Wählen Sie auf der Seite Unternehmenskonto verknüpfen die Option Facebook-Portal starten aus. Ein neues Anmeldefenster von Meta wird angezeigt.
4. Geben Sie im Meta-Anmeldefenster Ihre Facebook-Kontoanmeldedaten ein.

   Wählen Sie auf der Seite mit dem WhatsApp Unternehmenskonto die Option WhatsAppTelefonnummer hinzufügen aus. Wählen Sie auf der Seite WhatsApp Telefonnummer hinzufügen die Option Facebook-Portal starten aus. Ein neues Anmeldefenster von Meta wird angezeigt.
5. Geben Sie im Meta-Anmeldefenster Ihre Facebook-Kontoanmeldedaten ein.

6. Im Rahmen des Anmeldevorgangs gewähren Sie AWS End User Messaging Social Zugriff auf Ihr WhatsApp Geschäftskonto (WABA). Sie gestatten AWS End User Messaging Social auch, Ihnen Nachrichten in Rechnung zu stellen. Klicken Sie auf Weiter.
7. Wählen Sie für ein Meta-Geschäftskonto ein vorhandenes Meta-Geschäftskonto aus oder erstellen Sie ein Meta-Geschäftskonto.

    a. (Optional) Wenn Sie ein Meta Business-Konto erstellen müssen, gehen Sie wie folgt vor:

    b. Geben Sie unter Firmenname den Namen Ihres Unternehmens ein.

    c. Geben Sie für Unternehmenswebsite oder Profilseite entweder die URL für die Website Ihres Unternehmens ein, oder wenn Ihr Unternehmen keine Website hat, geben Sie die URL zu Ihrer Social-Media-Seite ein.

    d. Wählen Sie unter Land das Land aus, in dem Ihr Unternehmen ansässig ist.

    e. (Optional) Wählen Sie Adresse hinzufügen und geben Sie die Adresse Ihres Unternehmens ein.
8. Wählen Sie Weiter.
9. Wählen Sie unter WhatsApp Geschäftskonto auswählen ein vorhandenes WhatsApp Geschäftskonto (WABA) aus, oder wenn Sie ein Konto erstellen müssen, wählen Sie „ WhatsApp Geschäftskonto erstellen“.

    Wählen Sie unter WhatsApp Unternehmensprofil erstellen oder auswählen ein vorhandenes WhatsApp Unternehmensprofil oder Neues WhatsApp Unternehmensprofil erstellen aus.
10. Wählen Sie Weiter.
11. Geben Sie unter Unternehmensprofil erstellen die folgenden Informationen ein:

    - Geben Sie unter WhatsApp Geschäftskontoname einen Namen für Ihr Konto ein. Dieses Feld ist nicht für Kunden bestimmt.
    - Geben Sie unter Anzeigename für das WhatsApp Unternehmensprofil den Namen ein, der Ihren Kunden angezeigt werden soll, wenn sie eine Nachricht von Ihnen erhalten. Wir empfehlen, dass Sie Ihren Firmennamen als Anzeigenamen verwenden. Der Name wird von Meta überprüft und muss den Regeln für WhatsApp Anzeigenamen entsprechen. Um einen Markennamen verwenden zu können, der sich von Ihrem Firmennamen unterscheidet, muss ein extern veröffentlichter Zusammenhang zwischen Ihrem Unternehmen und der Marke bestehen. Diese Assoziation muss auf Ihrer Website und auf der Marke, die auf der Website des Anzeigenamens dargestellt wird, angezeigt werden.

Sobald Sie die Registrierung abgeschlossen haben, führt Meta eine Überprüfung Ihres Anzeigenamens durch. Meta sendet Ihnen eine E-Mail, in der Sie darüber informiert werden, ob der Anzeigename genehmigt oder abgelehnt wurde. Wenn dein Anzeigename abgelehnt wird, wird dein Nachrichtenlimit pro Tag herabgesetzt und du könntest deine Verbindung beenden. WhatsApp

> **Important**
>
> Um deinen Anzeigenamen zu ändern, musst du ein Ticket beim Meta-Support erstellen.

- Wählen Sie unter Zeitzone die Zeitzone aus, in der sich das Unternehmen befindet.
- Wählen Sie unter Kategorie eine Kategorie aus, die am besten zu Ihrem Unternehmen passt. Kunden können sich Ihre Kategorie als Teil Ihrer Kontaktinformationen ansehen.
- Geben Sie unter Unternehmensbeschreibung eine Beschreibung Ihres Unternehmens ein. Kunden können Ihre Unternehmensbeschreibung als Teil Ihrer Kontaktinformationen einsehen.
- Geben Sie unter Website die Website Ihres Unternehmens ein. Kunden können Ihre Website als Teil Ihrer Kontaktinformationen aufrufen.
- Wählen Sie Weiter.

12. Geben Sie unter Telefonnummer hinzufügen für WhatsApp eine Telefonnummer eine Telefonnummer für die Registrierung ein. Diese Telefonnummer wird Ihren Kunden angezeigt, wenn Sie ihnen eine Nachricht senden.
13. Wählen Sie unter Wählen Sie aus, wie Sie Ihre Nummer verifizieren möchten, entweder Textnachricht oder Telefonanruf.

    - Wenn Sie bereit sind, den Bestätigungscode zu erhalten, wählen Sie Weiter.
    - Geben Sie den Bestätigungscode ein und wählen Sie dann Weiter.

14. Sobald Ihre Nummer verifiziert wurde, können Sie Weiter wählen, um das Fenster von Meta aus zu schließen.
15. Erweitern Sie für WhatsApp Geschäftskonten die Option Tags — optional, um Ihrem WhatsApp Geschäftskonto Stichwörter hinzuzufügen.

    Tags sind Schlüssel- und Wertepaare, die Sie optional auf Ihre AWS Ressourcen anwenden können, um den Zugriff oder die Nutzung zu kontrollieren. Wählen Sie Neues Tag hinzufügen und geben Sie ein Schlüssel-Wert-Paar ein, das angehängt werden soll.

16. Ein WhatsApp Geschäftskonto kann über ein einziges Nachrichten- und Ereignisziel verfügen, um Ereignisse für das WhatsApp Geschäftskonto und alle mit dem Geschäftskonto verknüpften Ressourcen zu protokollieren. WhatsApp Um die Ereignisprotokollierung in Amazon SNS zu aktivieren, einschließlich der Protokollierung des Empfangs einer Kundennachricht, müssen Sie die Veröffentlichung von Nachrichten und Ereignissen aktivieren. Weitere Informationen finden Sie unter Nachrichten- und Ereignisziele in AWS End User Messaging Social.

    > **Important**
    >
    > Um auf Kundennachrichten antworten zu können, müssen Sie die Veröffentlichung von Nachrichten und Ereignissen aktivieren.

    Aktivieren Sie im Abschnitt Details zum Ziel von Nachrichten und Ereignissen die Option Veröffentlichen von Ereignissen. Wählen Sie für Amazon SNS entweder Neues Amazon SNS SNS-Standardthema und geben Sie einen Namen in das Feld Themenname ein, oder wählen Sie Bestehendes Amazon SNS SNS-Standardthema und wählen Sie ein Thema aus der Dropdownliste Thema arn aus.

17. Unter Telefonnummern:

    Für jede Telefonnummer unter WhatsApp Telefonnummern:

    a. Geben Sie zur Überprüfung der Telefonnummer die bestehende PIN oder einen neuen PIN-Code ein. Um eine verlorene oder vergessene PIN zurückzusetzen, folgen Sie den Anweisungen unter PIN aktualisieren in der WhatsApp Business Platform Cloud API-Referenz.

    b. Für zusätzliche Einstellungen:

        i. Wählen Sie für Datenlokalisierungsregion — optional eine der Regionen von Meta aus, in der Sie Ihre Daten im Ruhezustand speichern möchten. Weitere Informationen zu den Datenschutzrichtlinien von Meta finden Sie unter Datenschutz und Sicherheit und Cloud API Local Storage in der WhatsApp Business Platform Cloud API-Referenz.

        ii. Tags sind Schlüssel- und Wertepaare, die Sie optional auf Ihre AWS Ressourcen anwenden können, um den Zugriff oder die Nutzung zu kontrollieren. Wählen Sie Neues Tag hinzufügen und geben Sie ein Schlüssel-Wert-Paar ein, das angehängt werden soll.

18. Ein WhatsApp Geschäftskonto kann über ein einziges Nachrichten- und Ereignisziel verfügen, um Ereignisse für das WhatsApp Geschäftskonto und alle mit dem Geschäftskonto verknüpften Ressourcen zu protokollieren. WhatsApp Um die Ereignisprotokollierung, einschließlich der Protokollierung des Empfangs einer Kundennachricht, zu aktivieren, müssen Sie das Veröffentlichen von Nachrichten und Ereignissen aktivieren. Weitere Informationen finden Sie unter Nachrichten- und Ereignisziele in AWS End User Messaging Social.

    > **Important**
    >
    > Sie müssen die Veröffentlichung von Nachrichten und Ereignissen aktivieren, um auf Kundennachrichten antworten zu können.

    Aktivieren Sie im Abschnitt Details zum Ziel von Nachrichten und Ereignissen die Option Veröffentlichen von Ereignissen.
19. Wählen Sie als Zieltyp entweder Amazon SNS oder Amazon Connect

    a. Um Ihre Ereignisse an ein Amazon SNS SNS-Ziel zu senden, geben Sie unter Thema ARN einen vorhandenen Themen-ARN ein. Beispiele für IAM-Richtlinien finden Sie unter IAM-Richtlinien für Amazon SNS SNS-Themen.

    b. Für Amazon Connect

        i. Wählen Sie für Connect-Instanz eine Instanz aus dem Drop-down-Menü aus.

        ii. Wählen Sie für Role ARN eine der folgenden Optionen aus:

            A. Bestehende IAM-Rolle auswählen — Wählen Sie eine bestehende IAM-Richtlinie aus der Dropdownliste „Bestehende IAM-Rollen“ aus. Beispiele für IAM-Richtlinien finden Sie unter IAM-Richtlinien für Amazon Connect.

            B. IAM-Rollen-ARN eingeben — Geben Sie den ARN der IAM-Richtlinie unter Vorhandenen IAM-Rollen-Arn verwenden ein. Beispiele für IAM-Richtlinien finden Sie unter IAM-Richtlinien für Amazon Connect.
20. Um die Einrichtung abzuschließen, wählen Sie Telefonnummer hinzufügen.

Nächste Schritte

Sobald Sie die Registrierung abgeschlossen haben, können Sie mit dem Senden von Nachrichten beginnen. Wenn Sie bereit sind, Nachrichten in großem Umfang zu versenden, schließen Sie die

Unternehmensverifizierung ab. Nachdem Ihr WhatsApp Unternehmenskonto und Ihre Konten für AWS End User Messaging Social miteinander verknüpft sind, finden Sie weitere Informationen zu den folgenden Themen:

- Erfahren Sie mehr über das Ereignisziel zum Protokollieren von Ereignissen und zum Empfangen eingehender Nachrichten.
- Erfahren Sie, wie Sie Nachrichtenvorlagen erstellen.
- Erfahren Sie, wie Sie eine Text- oder Mediennachricht senden.
- Erfahren Sie, wie Sie eine Nachricht empfangen können.
- Erfahre mehr über offizielle Geschäftskonten, um neben deinem Anzeigenamen ein grünes Häkchen zu haben und deinen Nachrichtendurchsatz zu erhöhen.

WhatsApp Geschäftskonto (WABA) in AWS End User Messaging Social

Mit einem WhatsApp Geschäftskonto (WABA) können Sie die WhatsApp Business Platform verwenden, um Nachrichten direkt an Ihre Kunden zu senden. Sie alle WABAs sind Teil Ihres Meta Business Portfolios. Ein WhatsApp Geschäftskonto enthält Ihre kundenorientierten Ressourcen wie Telefonnummer, Vorlagen und Geschäftskontaktinformationen. Eine WABA kann nur in einem AWS-Region existieren. Weitere Informationen zu WhatsApp Geschäftskonten finden Sie unter WhatsAppGeschäftskonten in der WhatsApp Business Platform Cloud API-Referenz.

Important

Arbeiten mit Meta/ WhatsApp

- Ihre Nutzung der WhatsApp Business Solution unterliegt den Bedingungen der Nutzungsbedingungen für Unternehmen, den Nutzungsbedingungen für WhatsApp Business Solution, der WhatsApp WhatsApp Business Messaging-Richtlinie, den WhatsApp Messaging-Richtlinien und allen anderen Bestimmungen, Richtlinien oder Richtlinien, auf die verwiesen wird. Diese können von Zeit zu Zeit aktualisiert werden.
- Meta oder WhatsApp kann Ihnen jederzeit die Nutzung der WhatsApp Business Solution verbieten.
- Sie müssen ein WhatsApp Geschäftskonto (WABA) bei Meta und einrichten. WhatsApp
- Sie müssen ein Business Manager-Konto bei Meta erstellen und es mit Ihrer WABA verknüpfen.
- Sie müssen uns die Kontrolle über Ihre WABA gewähren. Auf Ihren Wunsch hin übertragen wir Ihnen die Kontrolle über Ihre WABA in angemessener und zeitnaher Weise zurück und verwenden dabei die Methoden, die Meta uns zur Verfügung stellt.
- Im Zusammenhang mit Ihrer Nutzung der WhatsApp Business Solution werden Sie keine Inhalte, Informationen oder Daten übermitteln, die gemäß den geltenden Gesetzen oder Vorschriften Schutzmaßnahmen oder Vertriebsbeschränkungen unterliegen.
- WhatsAppDie Preise für die Nutzung der WhatsApp Business Solution finden Sie unter https://developers.facebook.com/docs/whatsapp/pricing.

Themen

Sehen Sie sich ein WhatsApp Geschäftskonto (WABA) in End User Messaging Social an AWS

Sie können die mit Ihrem verknüpft WABA einsehen. AWS-Konto

Um die mit Ihrem Konto verknüpften WABA anzuzeigen

1. Öffnen Sie die AWS End User Messaging Social-Konsole unter https://console.aws.amazon.com/social-messaging/.
2. Wählen Sie unter Unternehmenskonten eine WABA aus.
3. Sehen Sie sich auf der Registerkarte Telefonnummern Ihre Telefonnummer, den Anzeigenamen, die Qualitätsbewertung und die Anzahl der geschäftlich initiierten Konversationen an, die Sie für diesen Tag noch übrig haben.

   Sehen Sie sich auf der Registerkarte Veranstaltungsziele Ihr Veranstaltungsziel an. Folgen Sie den Anweisungen unter, um Ihr Veranstaltungsziel zu bearbeitenNachrichten- und Ereignisziele in AWS End User Messaging Social.

   Wählen Sie auf dem Tab Vorlagen die Option Nachrichtenvorlagen verwalten aus, um Ihre WhatsApp Vorlagen über Meta zu bearbeiten. Jede WABA hat ein Limit von 250 Vorlagen.

   Auf der Registerkarte „Tags“ können Sie Ihre WABA-Ressourcen-Tags verwalten.

Fügen Sie ein WhatsApp Geschäftskonto (WABA) in AWS End User Messaging Social hinzu

Fügen Sie Ihrem Konto eine neue WABA hinzu, wenn Sie bereits ein WhatsApp Unternehmensprofil haben. Im Rahmen der Erstellung einer neuen WABA müssen Sie der WABA eine Telefonnummer hinzufügen.

- Gehen Sie wie folgt vor, um Ihrem Konto eine neue WABA hinzuzufügen: Erste Schritte mit AWS End User Messaging Social
  - Wählen Sie in Schritt 8 Ihr WhatsApp Unternehmensprofil und anschließend die Option Neues WhatsApp Geschäftskonto erstellen aus.

Grundlegendes WhatsApp zu Geschäftskontotypen

Ihr WhatsApp Geschäftskonto bestimmt, wie Sie Ihren Kunden gegenüber auftreten. Wenn Sie ein WhatsApp Konto erstellen, wird Ihr Konto ein Geschäftskonto sein. WhatsApp hat zwei Arten von Geschäftskonten:

- Geschäftskonto: WhatsApp überprüft die Echtheit jedes Kontos auf der WhatsApp Geschäftsplattform. Wenn ein Geschäftskonto den Geschäftsverifizierungsprozess abgeschlossen hat, ist der Unternehmensname für alle Benutzer sichtbar. Diese Funktion hilft Benutzern dabei, verifizierte Geschäftskonten zu identifizieren WhatsApp.
- Offizielles Geschäftskonto: Neben den Vorteilen eines Geschäftskontos verfügt ein offizielles Geschäftskonto auch über ein grünes Häkchen im Profil und in den Kopfzeilen des Chat-Threads.

  Für die Genehmigung eines WhatsApp offiziellen Geschäftskontos (OBA) ist der Nachweis erforderlich, dass das Unternehmen bei den Verbrauchern bekannt und anerkannt ist, z. B. in Form von Artikeln, Blogbeiträgen oder unabhängigen Rezensionen. Die Zulassung eines WhatsApp OBA ist nicht garantiert, auch wenn das Unternehmen die erforderlichen Unterlagen vorlegt. Das Genehmigungsverfahren steht unter dem Vorbehalt der Überprüfung und Genehmigung durch WhatsApp. WhatsApp gibt die spezifischen Kriterien, die sie für die Bewertung und Genehmigung von Anträgen auf offizielle Geschäftskonten verwenden, nicht öffentlich bekannt. Die Unternehmen, die ein WhatsApp OBA beantragen, müssen ihren Ruf und ihre Anerkennung nachweisen, die endgültige Genehmigung liegt jedoch im Ermessen von WhatsApp.

Wenn Sie ein WhatsApp Konto erstellen, wird Ihr Konto zu einem Geschäftskonto. Sie können Ihren Kunden Informationen über Ihr Unternehmen wie Website, Adresse und Öffnungszeiten zur Verfügung stellen. Bei Unternehmen, die die WhatsApp Unternehmensverifizierung nicht abgeschlossen haben, wird der Anzeigename in der Kontaktansicht als kleiner Text neben der Telefonnummer angezeigt, nicht in der Chat-Liste oder im Einzelchat. Sobald die Meta-Unternehmensverifizierung abgeschlossen ist, wird der Anzeigename des WhatsApp Absenders in der Chat-Liste und in den einzelnen Chat-Threads angezeigt.

Weitere Ressourcen

- Weitere Informationen zum Geschäftskonto und zum offiziellen Geschäftskonto finden Sie unter Geschäftskonten in der WhatsApp Business Platform Cloud API-Referenz.
- Weitere Informationen zum Prozess der Unternehmensverifizierung finden Sie unter Unternehmensverifizierung in der WhatsApp Business Platform Cloud API-Referenz.

Telefonnummern in AWS End User Messaging Social

Alle WhatsApp Geschäftskonten enthalten eine oder mehrere Telefonnummern, die zur Überprüfung Ihrer Identität verwendet werden, WhatsApp und werden als Teil Ihrer Absenderidentität verwendet. Sie können einem WhatsApp Geschäftskonto (WABA) mehrere Telefonnummern zuordnen und jede Telefonnummer für eine andere Marke verwenden.

Themen

Überlegungen zur Verwendung von Telefonnummern mit einem WhatsApp Geschäftskonto

Wenn Sie eine Telefonnummer mit Ihrem WhatsApp Geschäftskonto (WABA) verknüpfen, sollten Sie Folgendes berücksichtigen:

- Telefonnummern können jeweils nur mit einer WABA verknüpft werden.
- Die Telefonnummer kann weiterhin für SMS, MMS und Sprachanrufe verwendet werden.
- Jede Telefonnummer hat eine Qualitätsbewertung von Meta.

Gehen Sie wie folgt vor, um eine SMS-fähige Telefonnummer über AWS End User Messaging SMS zu erhalten:

1. Stellen Sie sicher, dass das Land oder die Region für die Telefonnummer bidirektionale SMS unterstützt.
2. Fordere die Telefonnummer an. Je nach Land oder Region müssen Sie die Telefonnummer möglicherweise registrieren.

3. Aktivieren Sie bidirektionale SMS-Nachrichten für die Telefonnummer. Sobald die Einrichtung abgeschlossen ist, werden Ihre eingehenden SMS-Nachrichten an ein Veranstaltungsziel gesendet.

Eine Telefonnummer zu einem WhatsApp Geschäftskonto hinzufügen (WABA)

Sie können einem bestehenden WhatsApp Geschäftskonto (WABA) Telefonnummern hinzufügen oder eine neue WABA für die Telefonnummer erstellen.

Voraussetzungen

Bevor Sie beginnen, müssen die folgenden Voraussetzungen erfüllt sein:

- Die Telefonnummer muss in der Lage sein, entweder eine SMS oder einen Einmalpasscode (OTP) per Spracheingabe zu empfangen. Dies ist die Telefonnummer, die zu Ihrer WABA hinzugefügt wird.
- Die Telefonnummer darf nicht mit einer anderen WABA verknüpft sein.

Die folgenden Voraussetzungen müssen erfüllt sein, um entweder ein Amazon SNS SNS-Thema oder eine Amazon Connect Connect-Instance als Nachrichten- und Ereignisziel verwenden zu können.

Amazon SNS-Thema

- Ein Amazon SNS SNS-Thema wurde erstellt und Berechtigungen wurden hinzugefügt.

> **Note**
>
> Amazon-SNS-FIFO-Themen werden nicht unterstützt.

- (Optional) Um ein Amazon SNS SNS-Thema zu verwenden, das mit AWS KMS Schlüsseln verschlüsselt ist, müssen Sie AWS End User Messaging Social-Berechtigungen für die bestehende Schlüsselrichtlinie gewähren.

Amazon Connect Connect-Instanz

- Eine Amazon Connect Connect-Instanz wurde erstellt und Berechtigungen wurden hinzugefügt.

Fügen Sie einer WABA eine Telefonnummer hinzu

Um eine neue Telefonnummer zu Ihrer bestehenden WABA hinzuzufügen

1. Öffnen Sie die AWS End User Messaging Social-Konsole unter https://console.aws.amazon.com/social-messaging/.
2. Wählen Sie Geschäftskonten und dann WhatsAppTelefonnummer hinzufügen aus.
3. Wählen Sie auf der Seite WhatsApp Telefonnummer hinzufügen die Option Facebook-Portal starten aus. Ein neues Anmeldefenster von Meta wird angezeigt.
4. Geben Sie im Meta-Anmeldefenster die Anmeldeinformationen Ihres Meta-Entwicklerkontos ein und wählen Sie Ihr Geschäftsportfolio aus.
5. Wählen Sie die WABA und das WhatsApp Unternehmensprofil aus, denen Sie die Telefonnummer hinzufügen möchten.
6. Wählen Sie Weiter.
7. Geben Sie unter Telefonnummer hinzufügen für WhatsApp eine Telefonnummer eine Telefonnummer für die Registrierung ein. Diese Telefonnummer wird Ihren Kunden angezeigt, wenn Sie ihnen eine Nachricht senden.
8. Wählen Sie unter Wählen Sie aus, wie Sie Ihre Nummer verifizieren möchten, entweder Textnachricht oder Telefonanruf.
9. Wenn Sie bereit sind, den Bestätigungscode zu erhalten, wählen Sie Weiter
10. Geben Sie den Bestätigungscode ein und wählen Sie dann Weiter. Sobald Ihre Nummer verifiziert wurde, können Sie Weiter wählen, um das Fenster von Meta aus zu schließen.
11. Unter WhatsApp Telefonnummern:

    a. Geben Sie zur Bestätigung der Telefonnummer die bestehende PIN oder einen neuen PIN-Code ein. Um eine verlorene oder vergessene PIN zurückzusetzen, folgen Sie den Anweisungen unter PIN aktualisieren in der WhatsApp Business Platform Cloud API-Referenz.

    b. Für zusätzliche Einstellungen:

i. Wählen Sie unter Datenlokalisierungsregion — optional eine der Regionen von Meta aus, in der Sie Ihre Daten im Ruhezustand speichern möchten. Weitere Informationen zu den Datenschutzrichtlinien von Meta finden Sie unter Datenschutz und Sicherheit und Cloud API Local Storage in der WhatsAppBusiness Platform Cloud API-Referenz.

ii. Tags sind Schlüssel- und Wertepaare, die Sie optional auf Ihre AWS Ressourcen anwenden können, um den Zugriff oder die Nutzung zu kontrollieren. Wählen Sie Neues Tag hinzufügen und geben Sie ein Schlüssel-Wert-Paar ein, das angehängt werden soll.

12. Ein WhatsApp Geschäftskonto kann über ein einziges Nachrichten- und Ereignisziel verfügen, um Ereignisse für das WhatsApp Geschäftskonto und alle mit dem Geschäftskonto verknüpften Ressourcen zu protokollieren. WhatsApp Um die Ereignisprotokollierung, einschließlich der Protokollierung des Empfangs einer Kundennachricht, zu aktivieren, aktivieren Sie die Option Nachrichten und Ereignisse veröffentlichen. Weitere Informationen finden Sie unter Nachrichten- und Ereignisziele in AWS End User Messaging Social.

> **Important**
>
> Sie müssen die Veröffentlichung von Nachrichten und Ereignissen aktivieren, um auf Kundennachrichten antworten zu können.

Aktivieren Sie im Abschnitt Details zum Ziel von Nachrichten und Ereignissen die Option Veröffentlichen von Ereignissen.

13. Wählen Sie als Zieltyp entweder Amazon SNS oder Amazon Connect

a. Um Ihre Ereignisse an ein Amazon SNS SNS-Ziel zu senden, geben Sie unter Thema ARN einen vorhandenen Themen-ARN ein. Beispiele für IAM-Richtlinien finden Sie unter IAM-Richtlinien für Amazon SNS SNS-Themen.

b. Für Amazon Connect

i. Wählen Sie für Connect-Instanz eine Instanz aus dem Drop-down-Menü aus.

ii. Wählen Sie für die bidirektionale Kanalrolle eine der folgenden Optionen aus:

A. Bestehende IAM-Rolle auswählen — Wählen Sie eine bestehende IAM-Richtlinie aus der Drop-down-Liste „Bestehende IAM-Rollen“ aus. Beispiele für IAM-Richtlinien finden Sie unter IAM-Richtlinien für Amazon Connect.

B. IAM-Rollen-ARN eingeben — Geben Sie den ARN der IAM-Richtlinie unter Vorhandenen IAM-Rollen-Arn verwenden ein. Beispiele für IAM-Richtlinien finden Sie unter IAM-Richtlinien für Amazon Connect.

14. Um die Einrichtung abzuschließen, wählen Sie Telefonnummer hinzufügen.

Den Status einer Telefonnummer anzeigen

Um Nachrichten in AWS End User Messaging Social senden zu können, muss der Status der Telefonnummer Aktiv sein.

1. Öffnen Sie die AWS End User Messaging Social-Konsole unter https://console.aws.amazon.com/social-messaging/.
2. Wählen Sie Phone numbers (Telefonnummern) aus.
3. Im Bereich Telefonnummern enthält die Spalte Status den Status der einzelnen Telefonnummern.

> **Note**
>
> Wenn der Status einer Telefonnummer Unvollständige Einrichtung lautet, können Sie die Telefonnummer auswählen und dann Vollständige Einrichtung wählen, um die Einrichtung der Telefonnummer abzuschließen.

Die ID einer Telefonnummer in AWS End User Messaging Social anzeigen

Um Nachrichten mit dem senden zu können AWS CLI, benötigen Sie die Rufnummer-ID, um die Telefonnummer zu identifizieren, die beim Senden verwendet werden soll.

1. Öffnen Sie die AWS End User Messaging Social-Konsole unter https://console.aws.amazon.com/social-messaging/.
2. Wählen Sie Phone numbers (Telefonnummern) aus.
3. Wählen Sie im Bereich Telefonnummern eine Telefonnummer aus.
4. Der Abschnitt mit den Telefonnummerdetails enthält die Rufnummer-ID der Telefonnummer.

Erhöhen Sie die Beschränkungen für Messaging-Konversationen WhatsApp

Nachrichtenlimits beziehen sich auf die maximale Anzahl geschäftlich initiierter Konversationen, die eine geschäftliche Telefonnummer innerhalb von 24 Stunden eröffnen kann. Geschäftstelefonnummern sind zunächst auf 250 geschäftlich initiierte Konversationen innerhalb eines Umzugszeitraums von 24 Stunden begrenzt. Dieses Limit kann von Meta auf der Grundlage der Qualitätsbewertung Ihrer Nachrichten und der Anzahl der von Ihnen gesendeten Nachrichten erhöht werden. Von Unternehmen initiierte Konversationen können nur Vorlagennachrichten verwenden.

Wenn ein Kunde Ihnen eine Nachricht sendet, öffnet sich ein 24-Stunden-Servicefenster. Während dieser Zeit können Sie alle Nachrichtentypen versenden.

Sie können Ihr Nachrichtenlimit selbst auf 1.000 Nachrichten erhöhen, indem Sie die folgenden Richtlinien befolgen:

- Ihre geschäftliche Telefonnummer muss den Status Aktiv haben.
- Wenn Ihre Geschäftstelefonnummer eine schlechte Qualitätsbewertung hat, kann sie weiterhin auf 250 geschäftlich initiierte Konversationen pro Tag begrenzt werden, bis sich die Qualitätsbewertung verbessert.
- Beantragen Sie eine Unternehmensverifizierung. Wenn Ihr Unternehmen zugelassen ist, wird die Nachrichtenqualität analysiert, um festzustellen, ob Ihre Nachrichtenaktivitäten eine Erhöhung Ihres Nachrichtenlimits rechtfertigen. Basierend auf der Analyse wird Ihr Antrag auf Erhöhung des Nachrichtenlimits von Meta entweder genehmigt oder abgelehnt.
- Beantragen Sie eine Identitätsprüfung. Wenn du die Identitätsprüfung abgeschlossen hast und deine Identität bestätigt ist, genehmigt Meta eine Erhöhung des Nachrichtenlimits.
- Eröffnen Sie innerhalb eines Umzugszeitraums von 30 Tagen 1.000 oder mehr geschäftlich initiierte Konversationen mithilfe einer Vorlage mit hoher Qualitätsbewertung. Sobald Sie den Schwellenwert von 1.000 Konversationen erreicht haben, wird Ihre Nachrichtenqualität analysiert, um festzustellen, ob Ihre Nachrichtenaktivitäten eine Erhöhung Ihres Nachrichtenlimits rechtfertigen. Ziel ist es, konsistent qualitativ hochwertige Nachrichten zu senden, um Ihr Nachrichtenlimit möglicherweise zu erhöhen.

Wenn du die Unternehmensverifizierung oder Identitätsprüfung abgeschlossen hast oder 1.000 oder mehr geschäftliche Konversationen eröffnet hast und du immer noch auf 250 geschäftlich initiierte Konversationen begrenzt bist, sende bei Meta eine Anfrage für ein Upgrade der Nachrichtenebene.

Wenn deine Geschäfts- oder Identitätsverifizierung abgelehnt wird, kannst du deine Chancen auf eine Genehmigung erhöhen, indem du qualitativ hochwertige Nachrichten sendest. Durch das Versenden qualitativ hochwertiger, gesetzeskonformer und optionaler Nachrichten können Ihre Nachrichtenaktivitäten und -qualität neu bewertet werden, was möglicherweise zu einer Verbesserung Ihrer Möglichkeiten für genehmigte Nachrichten führen kann.

Ihr Qualitätsfaktor für Nachrichten WhatsApp wird auf der Grundlage des jüngsten Nutzer-Feedbacks und der Interaktionen berechnet, wobei neueren Daten mehr Gewicht beigemessen wird. Dies hilft bei der Beurteilung der Gesamtqualität und Zuverlässigkeit Ihrer Nachrichten auf der Plattform.

Das Niveau der Nachrichtenlimits wird erhöht

- 1.000 von Unternehmen initiierte Konversationen
- 10.000 von Unternehmen initiierte Gespräche
- 100.000 von Unternehmen initiierte Gespräche
- Eine unbegrenzte Anzahl von geschäftlich initiierten Konversationen

Erhöhen Sie den Nachrichtendurchsatz in WhatsApp

Der Nachrichtendurchsatz ist die Anzahl der eingehenden und ausgehenden Nachrichten pro Sekunde (MPS) für eine Telefonnummer. Standardmäßig hat jede Telefonnummer einen MPS von 80. Meta kann deinen MPS auf 1.000 erhöhen, wenn du die folgenden Anforderungen erfüllst:

- Die Telefonnummer muss in der Lage sein, eine unbegrenzte Anzahl geschäftlich initiierter Konversationen zu senden
- Die Telefonnummer muss eine Qualitätsbewertung von mittel oder höher haben.

Grundlegendes zur Qualitätsbewertung von Telefonnummern in WhatsApp

Die Qualität Ihrer Telefonnummer und Nachrichten wird von Meta bestimmt. Ihr Qualitätsfaktor für Nachrichten basiert darauf, wie Ihre Nachrichten in den letzten sieben Tagen von Kunden empfangen wurden, wobei neuere Nachrichten stärker gewichtet wurden. Der Qualitätsfaktor für Nachrichten wird auf der Grundlage einer Kombination von Qualitätssignalen aus den Konversationen zwischen Ihnen und Ihren WhatsApp Benutzern berechnet. Zu diesen Signalen gehören Benutzerfeedback wie Blockierungen, Berichte und die Gründe, die Benutzer angeben, wenn sie ein Unternehmen

blockieren. Meta bewertet die Qualität Ihrer Nachrichten danach, wie gut sie bei Ihren Kunden ankommen WhatsApp, wobei der Schwerpunkt auf aktuellen Rückmeldungen und Interaktionen liegt.

WhatsApp Bewertungen der Qualität von Telefonnummern

- Grün: Hohe Qualität
- Gelb: Mittlere Qualität
- Rot: Niedrige Qualität

WhatsApp Status der Telefonnummer

- Verbunden: Sie können innerhalb Ihres Nachrichtenkontingents Nachrichten senden.
- Markiert: Die Qualität Ihrer Telefonnummer ist schlecht und muss verbessert werden. Wenn sich Ihre Qualität innerhalb von sieben Tagen nicht verbessert, wird Ihr Telefonnummernstatus auf Verbunden geändert, aber das Limit für geschäftlich initiierte Konversationen wird um eine Stufe gesenkt.
- Eingeschränkt: Sie haben Ihr Limit für geschäftlich initiierte Konversationen für den aktuellen Zeitraum von 24 Stunden erreicht. Sie können weiterhin auf eingehende Nachrichten antworten. Nach Ablauf der 24-Stunden-Frist können Sie erneut Nachrichten senden.

Qualitätsbewertung einer Telefonnummer anzeigen

Folgen Sie diesen Anweisungen, um die Qualität einer Telefonnummer zu überprüfen.

1. Öffnen Sie die AWS End User Messaging Social-Konsole unter https://console.aws.amazon.com/social-messaging/.
2. Wählen Sie unter Geschäftskonten ein WhatsApp Geschäftskonto (WABA) aus.
3. Sehen Sie sich auf der Registerkarte Telefonnummern Ihre Telefonnummer, den Anzeigenamen, die Qualitätsbewertung und die Anzahl der geschäftlich initiierten Konversationen an, die Sie für diesen Tag noch übrig haben.

Nachrichtenvorlagen in AWS End User Messaging Social verwenden

> **Important**
>
> Ab dem 01.04.2025 blockiert Meta Vorlagen für Marketingnachrichten, die an die US-Landesvorwahl von gesendet werden. +1 Weitere Informationen finden Sie unter Nachrichtenlimits für Marketingvorlagen pro Benutzer in der WhatsAppBusiness Platform Cloud API-Referenz.

Sie können Nachrichtenvorlagen verwenden, um Nachrichtentypen zu erstellen, die Sie häufig verwenden, z. B. wöchentliche Newsletter oder Terminerinnerungen. Vorlagennachrichten sind die einzige Art von Nachricht, die an Kunden gesendet werden kann, die Ihnen noch keine Nachricht gesendet haben oder die Ihnen in den letzten 24 Stunden keine Nachricht gesendet haben.

Meta weist jeder Vorlage eine Qualitätsbewertung und einen Status zu. Die Qualitätsbewertung wirkt sich auf den Status einer Vorlage aus und senkt das Tempo oder die Versandrate einer Vorlage.

Vorlagen werden mit Ihrem WhatsApp Geschäftskonto (WABA) verknüpft, über den WhatsApp Manager verwaltet und von diesem überprüft. WhatsApp

Sie können die folgenden Vorlagentypen versenden:

- Textbasiert
- Medienbasiert
- Interaktive Nachricht
- Ortsbezogen
- Authentifizierungsvorlagen mit Schaltflächen für Einmalpasswörter
- Vorlagen für Nachrichten für mehrere Produkte

Meta bietet vorab genehmigte Mustervorlagen. Weitere Informationen finden Sie unter Beispielvorlagen für Nachrichten.

Weitere Informationen zu den Arten von Nachrichtenvorlagen finden Sie unter Nachrichtenvorlage in der WhatsApp Business Platform Cloud API-Referenz.

Nachrichtenvorlagen mit WhatsApp Manager verwenden

Verwenden Sie den WhatsAppManager, um den Status einer Vorlage zu erstellen, zu ändern oder zu überprüfen.

1. Öffnen Sie die AWS End User Messaging Social-Konsole unter https://console.aws.amazon.com/social-messaging/.
2. Wählen Sie Geschäftskonto und anschließend ein WABA aus.
3. Wählen Sie auf der Registerkarte Nachrichtenvorlagen die Option Nachrichtenvorlagen verwalten aus. Der WhatsAppManager öffnet ein neues Fenster, in dem Sie Ihre Vorlagen verwalten können, indem Sie Nachrichtenvorlagen auswählen.

Nachrichtenvorlagen mit der CreateWhatsAppMessageTemplate API erstellen

Mithilfe der End User Messaging Social API können Sie benutzerdefinierte WhatsApp Nachrichtenvorlagen erstellen. In diesem Thema wird beschrieben, wie Sie CreateWhatsAppMessageTemplatemit dem eine Vielzahl von WhatsApp Nachrichtenvorlagen erstellen können.

Komponenten von Nachrichtenvorlagen

WhatsApp Nachrichtenvorlagen können die folgenden Komponenten enthalten:

- Kopfzeile: Titeltext, der oben angezeigt wird
- Hauptteil: Inhalt der Hauptnachricht mit variablen Platzhaltern
- Fußzeile: Zusätzliche Informationen unten
- Schaltflächen: Anklickbare Elemente, die auf Folgendes verweisen URLs

In den folgenden Beispielen ersetzen Sie *`ENDPOINT`* und *`WABA_ID`* durch Ihre tatsächliche Endpunkt-URL und Ihre WhatsApp Geschäftskonto-ID.

Erstellen Sie eine einfache englische Utility-Vorlage

In diesem Beispiel wird eine Nachrichtenvorlage für ein Hilfsprogramm in englischer Sprache erstellt, die nur die BODY Komponente verwendet und keineHEADER,FOOTER, oder BUTTON -Komponenten enthält. Der Haupttext verwendet variable Platzhalter.

```
$ aws social-messaging create-whats-app-message-template --region us-east-1 --endpoint-
url ENDPOINT_URL \
--id WABA_ID \
--template-definition '{
    "name": "order_update_basic",
    "language": "en_US",
    "allow_category_change": true,
    "category": "UTILITY",
    "components": [
        {
            "type": "BODY",
            "text": "Hi {{1}}, your order #{{2}} has been shipped. Track your delivery
 below."
        }
    ]
}'
```

Erstellen Sie eine einfache englische Utility-Vorlage mit Schaltfläche

In diesem Beispiel wird eine Nachrichtenvorlage für ein Hilfsprogramm in englischer Sprache erstellt, die BODY auch BUTTON Komponenten enthält.

```
$ aws social-messaging create-whats-app-message-template --region us-east-1 --endpoint-
url ENDPOINT_URL \
--id WABA_ID \
--template-definition '{
    "name": "order_update_with_button",
    "language": "en_US",
    "allow_category_change": true,
    "category": "UTILITY",
    "components": [
        {
            "type": "BODY",
            "text": "Hi {{1}}, your order #{{2}} has been shipped. Track your delivery
 below."
        },
```

```
        {
            "type": "BUTTONS",
            "buttons": [
                {
                    "type": "URL",
                    "text": "Track Order",
                    "url": "https://example.com/track"
                }
            ]
        }
    ]
}'
```

Erstellen Sie eine komplexe englische Vorlage für Dienstprogrammnachrichten mit einer Kopfzeile, einem Hauptteil und einer Schaltfläche

In diesem Beispiel wird eine Nachrichtenvorlage für Hilfsprogramme in englischer Sprache erstelltHEADER, die BUTTON KomponentenBODY, und enthält.

```
$ aws social-messaging create-whats-app-message-template --region us-east-1 --endpoint-
url ENDPOINT_URL \
--id WABA_ID \
--template-definition '{
  "name": "account_creation_confirmation_3333",
  "category": "UTILITY",
  "language": "en_US",
  "status": "APPROVED",
  "components": [
    {
      "type": "HEADER",
      "format": "TEXT",
      "text": "Finalize account set-up"
    },
    {
      "type": "BODY",
      "text": "Hi {{1}},\n\nYour new account has been created successfully. \n\nPlease
 verify {{2}} to complete your profile.",
      "example": {
        "body_text": [
          [
            "John",
```

```
            "your email address"
          ]
        ]
      }
    },
    {
      "type": "BUTTONS",
      "buttons": [
        {
          "type": "URL",
          "text": "Verify account",
          "url": "https://www.example.com/"
        }
      ]
    }
  ]
}'
```

Erstellen Sie eine einfache Vorlage für Marketingnachrichten

In diesem Beispiel wird eine grundlegende Vorlage für Marketingnachrichten erstellt, die nur eine BODY Komponente enthält.

```
$ aws social-messaging create-whats-app-message-template --region us-east-1 --endpoint-
url ENDPOINT_URL \
--id WABA_ID \
--template-definition '{
  "id": "1290345849293233",
  "name": "holiday_special_1395238",
  "category": "MARKETING",
  "language": "en_US",
  "status": "PENDING",
  "components": [
    {
      "type": "BODY",
      "text": "Season's Greetings {{1}}!\n\nCelebrate {{2}} with amazing deals up to
 {{3}} off.\n\nPlus, get free gift wrapping on all orders above $50.",
      "example": {
        "body_text": [
          [
            "Pawan",
            "Christmas",
            "30%"
```

```
          ]
        ]
      }
    }
  ],
  "metaTemplateId": "1290345849293233"
}'
```

Erstellen Sie eine komplexe Vorlage für Marketingnachrichten

In diesem Beispiel wird eine Vorlage für Marketingnachrichten in englischer Sprache erstelltHEADER, die BUTTON KomponentenBODY, und enthält.

```
$ aws social-messaging create-whats-app-message-template --region us-east-1 \
--endpoint-url ENDPOINT_URL \
--id WABA_ID \
--template-definition '{
  "name": "summer_sale_1",
  "category": "MARKETING",
  "language": "en_US",
  "status": "APPROVED",
  "components": [
    {
      "type": "HEADER",
      "format": "TEXT",
      "text": "Summer Sale!"
    },
    {
      "type": "BODY",
      "text": "Hi {{1}}! Get {{2}} off all summer items. Shop now before stock runs
 out!"
    },
    {
      "type": "FOOTER",
      "text": "Valid until August 31st"
    },
    {
      "type": "BUTTONS",
      "buttons": [
        {
          "type": "URL",
          "text": "Shop Now",
          "url": "https://example.com/sale"
```

```
        }
      ]
    }
  ]
}'
```

Nächste Schritte

Sobald Sie eine Vorlage erstellt oder bearbeitet haben, müssen Sie sie zur Überprüfung einreichen WhatsApp. Die Überprüfung durch Meta kann bis zu 24 Stunden dauern. Meta sendet eine E-Mail an Ihren Business Manager-Administrator und aktualisiert den Status der Vorlage im WhatsApp Manager. Verwenden Sie den WhatsAppManager, um den Status Ihrer Vorlage zu überprüfen.

Grundlegendes zum Template-Pacing WhatsApp

Das Template Pacing ist eine von Meta verwendete Methode, die Zeit für frühzeitiges Feedback von Kunden zu neuen oder geänderten Vorlagen bietet. Es identifiziert und pausiert Vorlagen, die zu wenig Engagement oder Feedback erhalten, sodass Sie Zeit haben, den Inhalt der Vorlage anzupassen, bevor Sie sie an zu viele Kunden senden. Dadurch wird das Risiko verringert, dass sich negatives Kundenfeedback auf das Geschäft auswirkt. Wenn beispielsweise zu viele Kunden Ihre Nachricht „blockieren“ oder wenn Ihre Vorlage niedrige Leseraten aufweist, kann Ihre Qualitätsbewertung für Vorlagen herabgesetzt werden.

Das Template Pacing wirkt sich auf neu erstellte Vorlagen, Vorlagen, die nicht pausiert wurden, und Vorlagen ohne hohe Qualitätsbewertung aus. Das Template Pacing wird oft dadurch ausgelöst, dass es in der Vergangenheit Vorlagen mit schlechter Qualität gab oder pausiert wurde. Wenn das Tempo einer Vorlage festgelegt ist, werden Nachrichten, die diese Vorlage verwenden, normal bis zu einem bestimmten, von Meta festgelegten Schwellenwert gesendet. Danach werden weitere Nachrichten gespeichert, um Zeit für Kundenfeedback zu haben. Wenn das Feedback positiv ist, wird das Template Pacing dann erhöht. Wenn das Feedback negativ ist, wird das Template Pacing herabgesetzt, sodass Sie den Inhalt der Vorlage anpassen können. Weitere Informationen finden Sie unter Template Pacing in der WhatsApp Business Platform Cloud API-Referenz.

Holen Sie sich mit Manager Feedback zum niedrigeren Status einer WhatsApp Vorlage

Meta gibt Auskunft darüber, warum der Status einer Vorlage herabgesetzt wurde. Verwenden Sie das Feedback von Meta, um die Vorlage zu bearbeiten und zur erneuten Genehmigung einzureichen, eine andere Vorlage zu verwenden oder das Verhalten Ihrer Anwendung zu ändern. Wenn Sie die Nachrichtenvorlage bearbeiten und sie erneut genehmigt wird, verbessert sich ihre Qualitätsbewertung schrittweise, sofern sie nicht häufig negatives Feedback oder niedrige Leseraten erhält.

1. Öffnen Sie die AWS End User Messaging Social-Konsole unter https://console.aws.amazon.com/social-messaging/.
2. Wählen Sie Geschäftskonto und anschließend ein WABA aus.
3. Wählen Sie auf der Registerkarte Nachrichtenvorlagen die Option Nachrichtenvorlagen verwalten aus. Der WhatsAppManager wird in einem neuen Fenster geöffnet.
4. Wählen Sie Nachrichtenvorlagen und bewegen Sie den Mauszeiger über die Vorlage. Es sollte ein Tooltip mit Feedback dazu erscheinen, warum die Bewertung herabgesetzt wurde.

Informationen zum Status und zur Qualitätsbewertung einer Vorlage finden Sie in WhatsApp

Jeder Nachrichtenvorlage wird eine Qualitätsbewertung zugewiesen, die auf Nutzung, Kundenfeedback und Kundenbindung basiert. Eine Vorlage kann nur verwendet werden, wenn der Status Aktiv lautet, aber die Qualität bestimmt das Tempo der Vorlage. Wenn eine Nachrichtenvorlage durchweg negatives Feedback erhält oder ein geringes Engagement aufweist, führt dies zu einer Änderung des Status der Vorlage.

Meta ändert den Status oder die Qualitätsbewertung einer Vorlage automatisch auf der Grundlage von negativem oder positivem Feedback und Engagement. Wenn sich der Status Ihrer Vorlage ändert, erhalten Sie eine WhatsApp Manager-Benachrichtigung, eine E-Mail und eine Veranstaltungsbenachrichtigung. Verwenden Sie den WhatsAppManager, um den Status Ihrer Vorlage zu überprüfen.

Wenn Ihre Vorlage von abgelehnt wird WhatsApp, können Sie die Vorlage bearbeiten und erneut zur Genehmigung einreichen oder Einspruch bei WhatsApp einlegen. Weitere Informationen finden Sie unter Beschwerden in der WhatsApp Business Platform Cloud API-Referenz.

Status der Vorlage	Bewertung der Qualität	Bedeutung
Wird gerade überprüft		Die Nachrichtenvorlage wird überprüft. Der Vorgang kann bis zu 24 Stunden dauern.
Rejected (Abgelehnt)		Die Nachrichtenvorlage wurde abgelehnt, und Sie können Einspruch einlegen.
Aktiv	Ausstehend	Die Nachrichtenvorlage hat kein Qualitätsfeedback oder keine Informationen zur Leserate von Kunden erhalten, aber die Vorlage kann trotzdem zum Senden von Nachrichten verwendet werden.
Aktiv	Hoch	Die Nachrichtenvorlage hat kaum bis gar kein negatives Kundenfeedback erhalten und kann zum Senden von Nachrichten verwendet werden.
Aktiv	Mittelschwer	Die Nachrichtenvorlage hat negatives Feedback von Kunden oder niedrige Leseraten erhalten und ist möglicherweise pausiert oder deaktiviert.
Aktiv	Niedrig	Die Nachrichtenvorlage hat negatives Feedback von Kunden oder niedrige Leseraten erhalten. Nachricht envorlagen mit diesem

Status der Vorlage	Bewertung der Qualität	Bedeutung
		Status können verwendet werden, es besteht jedoch die Gefahr, dass sie pausiert oder deaktiviert werden. Wenn eine Vorlage den Status Active-Low annimmt, wird der Versand angehalten. Die erste Pause dauert drei Stunden, die zweite Pause sechs Stunden, und die nächste Pause deaktiviert die Vorlage.
Paused		Die Nachrichtenvorlage wurde aufgrund wiederkehrender negativer Rückmeldungen von Kunden oder aufgrund niedriger Leseraten pausiert.
Disabled		Die Nachrichtenvorlage wurde aufgrund wiederkehrender negativer Rückmeldungen von Kunden deaktiviert.
Einspruch erbeten		Ein Rechtsbehelf wurde beantragt.

Gründe, warum eine Vorlage abgelehnt wird WhatsApp

Wenn deine Nachrichtenvorlage von Meta geprüft und abgelehnt wird, erhältst du eine E-Mail, in der erklärt wird, warum die Vorlage abgelehnt wurde. Du kannst gegen die Ablehnung Berufung einlegen oder deine Nachrichtenvorlage ändern. Dies sind einige der häufigsten Gründe, warum Meta eine Nachrichtenvorlage ablehnen könnte:

- Variablenparameter enthalten Sonderzeichen wie #, $ oder%.

- Variablenparameter fehlen, haben nicht übereinstimmende geschweifte Klammern oder sind nicht sequentiell.
- Die Nachrichtenvorlage enthält Inhalte, die entweder gegen die WhatsApp Handelsrichtlinie oder die Geschäftsrichtlinie verstoßen. WhatsApps

Weitere Informationen finden Sie unter Häufige Ablehnungsgründe in der WhatsApp Business Platform Cloud API-Referenz.

Nachrichten- und Ereignisziele in AWS End User Messaging Social

Ein Ereignisziel ist ein Amazon SNS SNS-Thema oder eine Amazon Connect Connect-Instance, an die WhatsApp Ereignisse gesendet werden. Wenn Sie die Veröffentlichung von Ereignissen aktivieren, werden alle Ihre Sende- und Empfangsereignisse an die Nachricht und das Ziel des Ereignisses gesendet. Verwenden Sie Ereignisse, um den Status ausgehender Nachrichten und eingehender Kundenkommunikation zu überwachen, nachzuverfolgen und zu analysieren.

Jedes WhatsApp Geschäftskonto (WABA) kann ein Ereignisziel haben. Alle Ereignisse aus allen Ressourcen, die dem WhatsApp Geschäftskonto zugeordnet sind, werden an diesem Ereignisziel protokolliert. Sie könnten beispielsweise ein WhatsApp Geschäftskonto haben, dem drei Telefonnummern zugeordnet sind, und alle Ereignisse von diesen Telefonnummern werden an dem einen Ereignisziel protokolliert.

Themen

Fügen Sie eine Nachricht und ein Ereignisziel zu AWS End User Messaging Social hinzu

Wenn Sie die Veröffentlichung von Nachrichten und Ereignissen aktivieren, werden alle von Ihrem WhatsApp Geschäftskonto (WABA) generierten Ereignisse an das Amazon SNS SNS-Thema gesendet. Dies schließt Ereignisse für jede Telefonnummer ein, die einem WhatsApp Geschäftskonto zugeordnet ist. Ihrer WABA kann ein Amazon SNS SNS-Thema zugeordnet sein.

Voraussetzungen

Bevor Sie beginnen, müssen die folgenden Voraussetzungen erfüllt sein, um entweder ein Amazon SNS SNS-Thema oder eine Amazon Connect Connect-Instance als Nachrichten- und Ereignisziel verwenden zu können.

Amazon SNS-Thema

- Ein Amazon SNS SNS-Thema wurde erstellt und Berechtigungen wurden hinzugefügt.

> **Note**
>
> Amazon-SNS-FIFO-Themen werden nicht unterstützt.

- (Optional) Um ein Amazon SNS SNS-Thema zu verwenden, das mit AWS KMS Schlüsseln verschlüsselt ist, müssen Sie AWS End User Messaging Social-Berechtigungen für die bestehende Schlüsselrichtlinie gewähren.

Amazon Connect Connect-Instanz

- Eine Amazon Connect Connect-Instanz wurde erstellt und Berechtigungen wurden hinzugefügt.

Fügen Sie eine Nachricht und ein Ziel für ein Ereignis hinzu

1. Öffnen Sie die AWS End User Messaging Social-Konsole unter https://console.aws.amazon.com/social-messaging/.
2. Wählen Sie Geschäftskonto und anschließend ein WABA aus.
3. Wählen Sie auf der Registerkarte Ziel der Veranstaltung die Option Ziel bearbeiten aus.
4. Um ein Veranstaltungsziel zu aktivieren, wählen Sie Aktivieren aus.
5. Wählen Sie als Zieltyp entweder Amazon SNS oder Amazon Connect

    a. Um Ihre Ereignisse an ein Amazon SNS SNS-Ziel zu senden, geben Sie einen vorhandenen Themen-ARN in das Feld Themen-ARN ein. Beispiele für IAM-Richtlinien finden Sie unter IAM-Richtlinien für Amazon SNS SNS-Themen.

    b. Für Amazon Connect

        i. Wählen Sie für Connect-Instanz eine Instanz aus dem Drop-down-Menü aus.

        ii. Wählen Sie für die bidirektionale Kanalrolle eine der folgenden Optionen aus:

            A. Bestehende IAM-Rolle auswählen — Wählen Sie eine bestehende IAM-Richtlinie aus der Drop-down-Liste „Bestehende IAM-Rollen“ aus. Beispiele für IAM-Richtlinien finden Sie unter IAM-Richtlinien für Amazon Connect.

B. IAM-Rollen-ARN eingeben — Geben Sie den ARN der IAM-Richtlinie unter Vorhandenen IAM-Rollen-Arn verwenden ein. Beispiele für IAM-Richtlinien finden Sie unter IAM-Richtlinien für Amazon Connect.

6. Wählen Sie Änderungen speichern.

Themenrichtlinien für verschlüsselte Amazon SNS

Sie können Amazon SNS SNS-Themen verwenden, die mit AWS KMS Schlüsseln verschlüsselt sind, um eine zusätzliche Sicherheitsebene zu gewährleisten. Diese zusätzliche Sicherheit kann hilfreich sein, wenn Ihre Anwendung private oder sensible Daten verarbeitet. Weitere Informationen zur Verschlüsselung von Amazon SNS SNS-Themen mithilfe von AWS KMS Schlüsseln finden Sie unter Aktivieren der Kompatibilität zwischen Ereignisquellen von AWS Diensten und verschlüsselten Themen im Amazon Simple Notification Service Developer Guide.

> **Note**
>
> Amazon-SNS-FIFO-Themen werden nicht unterstützt.

In der Beispielanweisung werden die optionalen, aber empfohlenen `SourceArn` Bedingungen verwendet, `SourceAccount` um das Problem des verwirrten Stellvertreters zu vermeiden, und nur das Eigentümerkonto von AWS End User Messaging Social hat Zugriff. Weitere Informationen zum Problem des verwirrten Stellvertreters finden Sie unter Das Problem des verwirrten Stellvertreters im IAM-Benutzerhandbuch.

Der Schlüssel, den Sie verwenden, muss symmetrisch sein. Verschlüsselte Amazon SNS SNS-Themen unterstützen keine asymmetrischen Schlüssel AWS KMS .

Die Schlüsselrichtlinie muss geändert werden, damit AWS End User Messaging Social den Schlüssel verwenden kann. Folgen Sie den Anweisungen unter Ändern einer Schlüsselrichtlinie im AWS Key Management Service Entwicklerhandbuch, um der vorhandenen Schlüsselrichtlinie die folgenden Berechtigungen hinzuzufügen:

```
{
    "Effect": "Allow",
    "Principal": {
        "Service": "social-messaging.amazonaws.com"
    },
```

```
    "Action": [
        "kms:GenerateDataKey*",
        "kms:Decrypt"
    ],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "{ACCOUNT_ID}"
        },
        "ArnLike": {
          "aws:SourceArn": "arn:{PARTITION}:social-messaging:{REGION}:{ACCOUNT_ID}:*"
        }
     }
}
```

IAM-Richtlinien für Amazon SNS SNS-Themen

Um eine bestehende IAM-Rolle zu verwenden oder eine neue Rolle zu erstellen, fügen Sie dieser Rolle die folgende Richtlinie hinzu, damit AWS End User Messaging Social sie übernehmen kann. Informationen zum Ändern der Vertrauensstellung einer Rolle finden Sie unter Ändern einer Rolle im IAM-Benutzerhandbuch.

Im Folgenden finden Sie die Berechtigungsrichtlinie für die IAM-Rolle. Die Genehmigungsrichtlinie ermöglicht die Veröffentlichung in Amazon SNS SNS-Themen.

Nehmen Sie in der folgenden IAM-Berechtigungsrichtlinie die folgenden Änderungen vor:

- *{PARTITION}*Ersetzen Sie es durch die AWS Partition, in der Sie AWS End User Messaging Social verwenden.
- *{REGION}*Ersetzen Sie es durch AWS-Region die, in der Sie AWS End User Messaging Social verwenden.
- *{ACCOUNT}*Ersetzen Sie durch die eindeutige ID für Ihre AWS-Konto.
- *{TOPIC_NAME}*Ersetzen Sie es durch die Amazon SNS SNS-Themen, an die Nachrichten gesendet werden.

```
{
    "Effect": "Allow",
    "Principal": {
        "Service": [
          "social-messaging.amazonaws.com"
```

```
        ]
       },
    "Action": "sns:Publish",
    "Resource": "arn:{PARTITION}:sns:{REGION}:{ACCOUNT}:{TOPIC_NAME}"
}
```

IAM-Richtlinien für Amazon Connect

Wenn Sie möchten, dass AWS End User Messaging Social eine bestehende IAM-Rolle verwendet, oder wenn Sie eine neue Rolle erstellen, fügen Sie dieser Rolle die folgenden Richtlinien hinzu, damit AWS End User Messaging Social sie übernehmen kann. Informationen zum Ändern einer bestehenden Vertrauensstellung einer Rolle finden Sie unter Ändern einer Rolle im IAM-Benutzerhandbuch. Diese Rolle wird sowohl für das Senden von Ereignissen als auch für den Import von Telefonnummern aus AWS End User Messaging Social in Amazon Connect verwendet.

Gehen Sie wie folgt vor, um neue IAM-Richtlinien zu erstellen:

1. Erstellen Sie eine neue Berechtigungsrichtlinie, indem Sie den Anweisungen unter Erstellen von Richtlinien mit dem JSON-Editor im IAM-Benutzerhandbuch folgen.

   - Verwenden Sie in Schritt 5 die Berechtigungsrichtlinie für die IAM-Rolle, um die Veröffentlichung auf Amazon Connect zu ermöglichen.

     ```
     {
         "Version": "2012-10-17",
         "Statement": [
             {
                 "Sid": "AllowOperationsForEventDelivery",
                 "Effect": "Allow",
                 "Action": [
                     "connect:SendIntegrationEvent"
                 ],
                 "Resource": "*"
             },
             {
                 "Sid": "AllowOperationsForPhoneNumberImport",
                 "Effect": "Allow",
                 "Action": [
                     "connect:ImportPhoneNumber",
                     "social-messaging:GetLinkedWhatsAppBusinessAccountPhoneNumber",
                     "social-messaging:TagResource"
                 ],
     ```

```
            "Resource": "*"
        }
    ]
}
```

2. Erstellen Sie eine neue Vertrauensrichtlinie, indem Sie den Anweisungen unter Erstellen einer Rolle mithilfe benutzerdefinierter Vertrauensrichtlinien im IAM-Benutzerhandbuch folgen.

   a. Verwenden Sie in Schritt 4 die Vertrauensrichtlinie für die IAM-Rolle.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "social-messaging.amazonaws.com"
                ]
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

   b. Fügen Sie in Schritt 10 die Berechtigungsrichtlinie hinzu, die Sie im vorherigen Schritt erstellt haben.

Nächste Schritte

Sobald Sie Ihr Amazon SNS SNS-Thema eingerichtet haben, müssen Sie einen Endpunkt für das Thema abonnieren. Der Endpunkt beginnt, Nachrichten zu empfangen, die zu dem zugehörigen Thema veröffentlicht wurden. Weitere Informationen zum Abonnieren eines Themas finden Sie unter Amazon SNS SNS-Thema abonnieren im Amazon SNS SNS-Entwicklerhandbuch.

Nachrichten- und Ereignisformat in AWS End User Messaging Social

Das JSON-Objekt für ein Ereignis enthält den AWS Event-Header und die WhatsApp JSON-Payload. Eine Liste der Nutzdaten und Werte für WhatsApp JSON-Benachrichtigungen finden Sie in der

WhatsApp Business Platform Cloud API-Referenz unter Webhooks Notification Payload Reference und Message Status.

AWS Nachrichtenübermittlung an Endbenutzer in sozialen Netzwerken — Header

Das JSON-Objekt für ein Ereignis enthält den AWS Event-Header und WhatsApp JSON. Der Header enthält die AWS Identifikatoren sowie ARNs Ihr WhatsApp Geschäftskonto (WABA) und Ihre Telefonnummer.

```
{
  "context": {
    "MetaWabaIds": [
      {
        "wabaId": "1234567890abcde",
        "arn": "arn:aws:social-messaging:us-east-1:123456789012:waba/
fb2594b8a7974770b128a409e2example"
      }
    ],
    "MetaPhoneNumberIds": [
      {
        "metaPhoneNumberId": "abcde1234567890",
        "arn": "arn:aws:social-messaging:us-east-1:123456789012:phone-number-
id/976c72a700aac43eaf573ae050example"
      }
    ]
  },
  "whatsAppWebhookEntry": "{\"...JSON STRING....",
  "aws_account_id": "123456789012",
  "message_timestamp": "2025-01-08T23:30:43.271279391Z",
  "messageId": "6d69f07a-c317-4278-9d5c-6a84078419ec"
}
//Decoding the contents of whatsAppWebhookEntry
{
//WhatsApp notification payload
}
```

Im vorherigen Beispielereignis:

- *1234567890abcde*ist die WABA-ID von Meta.

- *abcde1234567890*ist die Rufnummer-ID von Meta.
- *fb2594b8a7974770b128a409e2example*ist die ID des WhatsApp Geschäftskontos (WABA).
- *976c72a700aac43eaf573ae050example*ist die ID der Telefonnummer.

WhatsApp JSON-Beispiel für den Empfang einer Nachricht

Im Folgenden wird der Ereignisdatensatz für eine eingehende Nachricht von angezeigt WhatsApp. Das von WhatsApp in empfangene JSON `whatsAppWebhookEntry` wird als JSON-Zeichenfolge empfangen und kann in JSON konvertiert werden. Eine Liste der Felder und ihrer Bedeutung finden Sie unter Webhooks Notification Payload Reference in der WhatsApp Business Platform Cloud API-Referenz.

```
{
  "context": {
    "MetaWabaIds": [
      {
        "wabaId": "1234567890abcde",
        "arn": "arn:aws:social-messaging:us-east-1:123456789012:waba/
fb2594b8a7974770b128a409e2example"
      }
    ],
    "MetaPhoneNumberIds": [
      {
        "metaPhoneNumberId": "abcde1234567890",
        "arn": "arn:aws:social-messaging:us-east-1:123456789012:phone-number-
id/976c72a700aac43eaf573ae050example"
      }
    ]
  },
  "whatsAppWebhookEntry": "{\"...JSON STRING....",
  "aws_account_id": "123456789012",
  "message_timestamp": "2025-01-08T23:30:43.271279391Z",
  "messageId": "6d69f07a-c317-4278-9d5c-6a84078419ec"
}
```

Sie können ein Tool wie jq verwenden, um die JSON-Zeichenfolge in JSON zu konvertieren. Das Folgende ist `whatsAppWebhookEntry` in JSON-Form:

```
{
  "id": "503131219501234",
```

```
  "changes": [
    {
      "value": {
        "messaging_product": "whatsapp",
        "metadata": {
          "display_phone_number": "14255550123",
          "phone_number_id": "46271669example"
        },
        "statuses": [
          {
            "id": "wamid.HBgLMTkxNzM5OTI3MzkVAgARGBJBMTM4NDdGRENEREI5Rexample",
            "status": "sent",
            "timestamp": "1736379042",
            "recipient_id": "01234567890",
            "conversation": {
              "id": "62374592e84cb58e52bdaed31example",
              "expiration_timestamp": "1736461020",
              "origin": {
                "type": "utility"
              }
            },
            "pricing": {
              "billable": true,
              "pricing_model": "CBP",
              "category": "utility"
            }
          }
        ]
      },
      "field": "messages"
    }
  ]
}
```


WhatsApp JSON-Beispiel für den Empfang einer Mediennachricht

Im Folgenden wird der Ereignisdatensatz für eine eingehende Mediennachricht angezeigt. Verwenden Sie den GetWhatsAppMessageMedia API-Befehl, um die Mediendatei abzurufen. Eine Liste der Felder und ihrer Bedeutung finden Sie unter Webhooks Notification Payload Reference


```
{
//AWS End User Messaging Social header
}
```

```
//Decoding the contents of whatsAppWebhookEntry
{
  "id": "365731266123456",
  "changes": [
    {
      "value": {
        "messaging_product": "whatsapp",
        "metadata": {
          "display_phone_number": "12065550100",
          "phone_number_id": "321010217760100"
        },
        "contacts": [
          {
            "profile": {
              "name": "Diego"
            },
            "wa_id": "12065550102"
          }
        ],
        "messages": [
          {
            "from": "14255550150",
            "id":
 "wamid.HBgLMTQyNTY5ODgzMDIVAgASGCBDNzBDRjM5MDU2ODEwMDkwREY4ODBDRDE0RjVGRkexample",
            "timestamp": "1723506230",
            "type": "image",
            "image": {
              "mime_type": "image/jpeg",
              "sha256": "BTD0xlqSZ7l02o+/upusiNStlEZhA/urkvKf143Uqjk=",
              "id": "530339869524171"
            }
          }
        ]
      },
      "field": "messages"
    }
  ]
}
```

WhatsApp Nachrichtenstatus

Wenn Sie eine Nachricht senden, erhalten Sie Statusmeldungen zu der Nachricht. Sie müssen die Ereignisprotokollierung aktivieren, um diese Benachrichtigungen zu erhalten, siehe Nachrichten- und Ereignisziele in AWS End User Messaging Social.

Status der Nachrichten

Die folgende Tabelle enthält mögliche Nachrichtenstatus.

Name des Status	Beschreibung
deleted	Der Kunde hat die Nachricht gelöscht, und Sie sollten die Nachricht auch löschen, wenn sie auf Ihren Server heruntergeladen wurde.
geliefert	Die Nachricht wurde erfolgreich an den Kunden zugestellt.
failed	Die Nachricht konnte nicht gesendet werden.
read	Der Kunde hat die Nachricht gelesen. Dieser Status wird nur gesendet, wenn der Kunde Lesebestätigungen aktiviert hat.
gesendet	Die Nachricht wurde gesendet, befindet sich aber noch im Transit.
warning	Die Nachricht enthält ein Element, das nicht verfügbar ist oder nicht existiert.

Weitere Ressourcen

Weitere Informationen finden Sie unter Nachrichtenstatus in der WhatsApp Business Platform Cloud API-Referenz.

Mediendateien hochladen, mit denen gesendet werden soll WhatsApp

Wenn Sie eine Mediendatei senden oder empfangen, muss sie in einem Amazon S3 S3-Bucket gespeichert und von dort hochgeladen oder abgerufen werden WhatsApp. Der Amazon S3 S3-Bucket muss sich im selben AWS-Konto und AWS-Region wie Ihr WhatsApp Geschäftskonto (WABA) befinden. Diese Anweisungen zeigen, wie Sie einen Amazon S3 S3-Bucket erstellen, eine Datei hochladen und die URL zu der Datei erstellen. Weitere Informationen zu Amazon S3 S3-Befehlen finden Sie unter Verwenden von High-Level-Befehlen (s3) mit der AWS-CLI. Weitere Informationen zur Konfiguration von finden Sie unter Konfiguration der AWS-CLI im AWS Command Line Interface Benutzerhandbuch und Erstellen eines Buckets und Hochladen von Objekten im Amazon S3 S3-Benutzerhandbuch. AWS CLI

> **Note**
>
> WhatsApp speichert Mediendateien 30 Tage lang, bevor sie gelöscht werden. Weitere Informationen finden Sie unter Upload Media in der WhatsApp Business Platform Cloud API-Referenz.

Sie können auch eine vorsignierte URL für die Mediendatei erstellen. Mit einer vorsignierten URL können Sie zeitlich begrenzten Zugriff auf Objekte gewähren und diese hochladen, ohne dass eine andere Partei über AWS Sicherheitsanmeldedaten oder -berechtigungen verfügen muss.

1. Verwenden Sie den Befehl create-bucket, um einen Amazon S3 S3-Bucket zu erstellen AWS CLI . Geben Sie in der Befehlszeile folgenden Befehl ein:

   ```
   aws s3api create-bucket --region 'us-east-1' --bucket BucketName
   ```

   Beim vorhergehenden Befehl:

   - Ersetzen Sie es *us-east-1* durch das AWS-Region , in dem sich Ihr WABA befindet.
   - *BucketName*Ersetzen Sie es durch den Namen des neuen Buckets.
2. Verwenden Sie den AWS CLI Befehl cp, um eine Datei in den Amazon S3 S3-Bucket zu kopieren. Geben Sie in der Befehlszeile folgenden Befehl ein:

```
aws s3 cp SourceFilePathAndName s3://BucketName/FileName
```

Beim vorhergehenden Befehl:

- *SourceFilePathAndName*Ersetzen Sie durch den Dateipfad und den Namen der zu kopierenden Datei.
- Ersetzen Sie *BucketName* durch den Namen Ihres Buckets.
- *FileName*Ersetzen Sie durch den Namen, der für die Datei verwendet werden soll.

Die URL, die beim Senden verwendet werden soll, lautet:

```
s3://BucketName/FileName
```

Um eine vorsignierte URL zu erstellen, ersetzen Sie sie durch Ihre eigenen Informationen. *user input placeholders*

```
aws s3 presign s3://amzn-s3-demo-bucket1/mydoc.txt --expires-in 604800 --region af-south-1 --endpoint-url https://s3.af-south-1.amazonaws.com
```

Die zurückgegebene URL wird wie folgt lauten: `https://amzn-s3-demo-bucket1.s3.af-south-1.amazonaws.com/mydoc.txt?{Headers}`

3. Laden Sie die Mediendatei WhatsApp mit dem post-whatsapp-message-mediaBefehl hoch. Bei erfolgreichem Abschluss gibt der Befehl den zurück*{MEDIA_ID}*, der für das Senden der Mediennachricht erforderlich ist.

```
aws socialmessaging post-whatsapp-message-media --origination-
phone-number-id {ORIGINATION_PHONE_NUMBER_ID}  --source-s3-file
 bucketName={BUCKET},key={MEDIA_FILE}
```

Gehen Sie im vorhergehenden Befehl wie folgt vor:

- *{ORIGINATION_PHONE_NUMBER_ID}*Ersetze es durch die ID deiner Telefonnummer.
- *{BUCKET}*Ersetzen Sie durch den Namen des Amazon S3 S3-Buckets.
- *{MEDIA_FILE}*Ersetzen Sie durch den Namen der Mediendatei.

Sie können den Upload auch mit einer Presign-URL durchführen, indem Sie `--source-s3-presigned-url` anstelle von `--source-s3-file` verwenden. Sie müssen das `Content-Type` `headers` Feld hinzufügen. Wenn Sie beide verwenden, `InvalidParameterException` wird ein zurückgegeben.

```
--source-s3-presigned-url headers={"Name":"Value"},url=https://BUCKET.s3.REGION/MEDIA_FILE
```

4. Bei erfolgreichem Abschluss *MEDIA_ID* wird der zurückgegeben. Das *MEDIA_ID* wird verwendet, um beim Senden einer Mediennachricht auf die Mediendatei zu verweisen.

Unterstützte Mediendateitypen und -größen in WhatsApp

Beim Senden oder Empfangen einer Mediennachricht muss der Dateityp unterstützt werden und die maximale Dateigröße darf nicht überschritten werden. Weitere Informationen finden Sie unter Unterstützte Medientypen in der WhatsApp Business Platform Cloud API-Referenz.

Mediendateitypen

Audioformate

Audio-Typ	Erweiterung	MIME-Typ	Max. Größe
AAC	.aac	Audio/AAC	16 MB
AMR	.amr	Audio/AMR	16 MB
MP3	.mp3	Audio/MPEG	16 MB
MP4 Audio	.m4a	Audio/MP4	16 MB
OGG-Audio	.ogg	Audio/OGG	16 MB

Formate der Dokumente

Dokumenttyp	Erweiterung	MIME-Typ	Max. Größe
Text	. Text	text/plain	100 MB

Dokumenttyp	Erweiterung	MIME-Typ	Max. Größe
Microsoft Excel	.xls, .xlsx	application/vnd.ms-excel, application/vnd.openxmlformats-officedocument.spreadsheetml.sheet	100 MB
Microsoft Word	.doc, .docx	application/msword, application/vnd.openxmlformats-officedocument.wordprocessingml.document	100 MB
Microsoft PowerPoint	.ppt, .pptx	application/vnd.ms-powerpoint, application/vnd.openxmlformats-officedocument.presentationml.presentation	100 MB
PDF	.pdf	application/pdf	100 MB

Image-Formate

Art des Bilds	Erweiterung	MIME-Typ	Max. Größe
JPEG	.jpeg	image/jpeg	5 MB
PNG	.png	image/png	5 MB

Formate von Aufklebern

Art des Aufklebers	Erweiterung	MIME-Typ	Max. Größe
Animierter Aufkleber	.webp	bild/webp	500 KB
Statischer Aufkleber	.webp	bild/webp	100 KB

Videoformate

Video-Typ	Erweiterung	MIME-Typ	Max. Größe
3 GPP	3,3 GP	Video/3GP	16 MB
MP4 Video	.mp4	Video/MP4	16 MB

WhatsApp Nachrichtentypen

In diesem Thema werden die unterstützten Nachrichtentypen und eine Beschreibung ihrer Verwendung aufgeführt. Eine Liste der Nachrichtentypen finden Sie unter Nachrichten in der WhatsApp Business Platform Cloud API-Referenz.

Art der Nachricht	Beschreibung
Text	Senden Sie eine Textnachricht oder URL an Ihren Kunden.
Medien	Senden Sie eine Audio-, Dokument-, Bild-, Aufkleber- oder Videodatei. Sie können auch Links zur Mediendatei senden.
Reaktion	Senden Sie ein Emoji als Reaktion auf eine Nachricht, z. B. einen Daumen hoch.
Vorlage	Senden Sie eine Vorlagennachricht.
Ort	Senden Sie einen Standort.
Kontakte	Senden Sie eine Kontaktkarte.
Interactive	Senden Sie eine interaktive Nachricht.

Weitere Ressourcen

Eine Liste der WhatsApp Nachrichtenobjekte finden Sie unter Nachrichten in der WhatsApp Business Platform Cloud API-Referenz.

Senden von Nachrichten WhatsApp mit AWS End User Messaging Social

Bevor Sie eine Nachricht senden, müssen Sie Ihr WhatsApp Geschäftskonto (WABA) einrichten und Ihr Benutzer muss sich dafür entscheiden, Nachrichten von Ihnen zu erhalten. Weitere Informationen finden Sie unter Einholen von Berechtigungen.

Wenn ein Benutzer Ihnen eine Nachricht sendet, wird ein 24-Stunden-Timer, ein sogenanntes Kundenservice-Fenster, gestartet oder aktualisiert. Alle Nachrichtentypen, mit Ausnahme von Vorlagennachrichten, können nur gesendet werden, wenn ein Kundendienstfenster zwischen Ihnen und dem Benutzer geöffnet ist. Vorlagennachrichten können jederzeit gesendet werden, sofern der Benutzer sich dafür entschieden hat, Nachrichten von Ihnen zu erhalten.

Für jede Nachricht, die Sie senden oder empfangen, wird ein Nachrichtenstatus generiert und an das Ereignisziel gesendet. Wenn sich Ihr Kunde nicht angemeldet hat WhatsApp, wird ein Ereignis mit dem Nachrichtenstatus generiert`fail`. Sie müssen eine Nachricht und ein Ziel für das Ereignis aktivieren, um den Nachrichtenstatus zu erhalten.

Eine Liste der Nachrichtentypen finden Sie unter Nachrichten in der WhatsApp Business Platform Cloud API-Referenz.

Important

Mit Meta/ arbeiten WhatsApp

- Ihre Nutzung der WhatsApp Business Solution unterliegt den Bedingungen der Nutzungsbedingungen für Unternehmen, den Nutzungsbedingungen für WhatsApp Business Solution, der WhatsApp WhatsApp Business Messaging-Richtlinie, den WhatsApp Messaging-Richtlinien und allen anderen Bestimmungen, Richtlinien oder Richtlinien, auf die verwiesen wird. Diese können von Zeit zu Zeit aktualisiert werden.
- Meta oder WhatsApp kann Ihnen jederzeit die Nutzung der WhatsApp Business Solution verbieten.
- Im Zusammenhang mit Ihrer Nutzung der WhatsApp Business Solution werden Sie keine Inhalte, Informationen oder Daten einreichen, die gemäß den geltenden Gesetzen oder Vorschriften Schutzmaßnahmen oder Vertriebsbeschränkungen unterliegen.

Themen

Beispiel für das Senden einer Vorlagennachricht in AWS End User Messaging Social

Weitere Informationen zu den Arten von Nachrichtenvorlagen, die gesendet werden können, finden Sie unter Nachrichtenvorlage in der WhatsApp Business Platform Cloud API-Referenz. Eine Liste der Nachrichtentypen, die gesendet werden können, finden Sie unter Nachrichten in der WhatsApp Business Platform Cloud API-Referenz.

Das folgende Beispiel zeigt, wie Sie eine Vorlage verwenden, um eine Nachricht an Ihren Kunden mithilfe von zu senden AWS CLI. Weitere Informationen zur Konfiguration von finden Sie unter Configure the AWS CLI im AWS Command Line Interface Benutzerhandbuch. AWS CLI

> **Note**
>
> Sie müssen die Base64-Kodierung angeben, wenn Sie AWS CLI Version 2 verwenden. Dies kann durch Hinzufügen des AWS CLI Parameters `--cli-binary-format raw-in-base64-out` oder Ändern der AWS CLI globalen Konfigurationsdatei geschehen. Weitere Informationen finden Sie `cli_binary_format`im AWS Command Line Interface User Guide für Version 2.

```
aws socialmessaging send-whatsapp-message --message
 '{"messaging_product":"whatsapp","to":"'{PHONE_NUMBER}'","type":"template","template":
{"name":"statement","language":{"code":"en_US"},"components":
[{"type":"body","parameters":[{"type":"text","text":"1000"}]}]}}' --origination-phone-
number-id {ORIGINATION_PHONE_NUMBER_ID} --meta-api-version v20.0
```

Gehen Sie im vorhergehenden Befehl wie folgt vor:

- *{PHONE_NUMBER}*Ersetzen Sie es durch die Telefonnummer Ihres Kunden.
- *{ORIGINATION_PHONE_NUMBER_ID}*Ersetze es durch die ID deiner Telefonnummer.

Das folgende Beispiel zeigt, wie eine Vorlagennachricht gesendet wird, die keine Komponenten enthält.

```
aws socialmessaging send-whatsapp-message --message '{"messaging_product":
 "whatsapp","to": "'{PHONE_NUMBER}'","type": "template","template":
 {"name":"simple_template","language": {"code": "en_US"}}}' --origination-phone-number-
id {ORIGINATION_PHONE_NUMBER_ID} --meta-api-version v20.0
```

- *{PHONE_NUMBER}*Ersetzen Sie es durch die Telefonnummer Ihres Kunden.
- *{ORIGINATION_PHONE_NUMBER_ID}*Ersetze es durch die ID deiner Telefonnummer.

Beispiel für das Senden einer Mediennachricht in AWS End User Messaging Social

Das folgende Beispiel zeigt, wie Sie mit dem eine Medienbotschaft an Ihren Kunden senden AWS CLI. Weitere Informationen zur Konfiguration von finden Sie unter Configure the AWS CLI im AWS Command Line Interface Benutzerhandbuch. AWS CLI Eine Liste der unterstützten Mediendateitypen finden Sie unterUnterstützte Mediendateitypen und -größen in WhatsApp.

> **Note**
>
> WhatsApp speichert Mediendateien 30 Tage lang, bevor sie gelöscht werden. Weitere Informationen finden Sie unter Upload Media in the WhatsApp Business Platform Cloud API-Referenz.

1. Laden Sie die Mediendatei in einen Amazon S3 S3-Bucket hoch. Weitere Informationen finden Sie unter Mediendateien hochladen, mit denen gesendet werden soll WhatsApp.
2. Laden Sie die Mediendatei WhatsApp mit dem post-whatsapp-message-mediaBefehl hoch. Nach erfolgreichem Abschluss gibt der Befehl den zurück*{MEDIA_ID}*, der für das Senden der Mediennachricht erforderlich ist.

   ```
   aws socialmessaging post-whatsapp-message-media --origination-
   phone-number-id {ORIGINATION_PHONE_NUMBER_ID}  --source-s3-file
    bucketName={BUCKET},key={MEDIA_FILE}
   ```

   Gehen Sie im vorhergehenden Befehl wie folgt vor:

- *{ORIGINATION_PHONE_NUMBER_ID}*Ersetze es durch die ID deiner Telefonnummer.
- *{BUCKET}*Ersetzen Sie durch den Namen des Amazon S3 S3-Buckets.
- *{MEDIA_FILE}*Ersetzen Sie durch den Namen der Mediendatei.

Sie können den Upload auch mit einer Presign-URL durchführen, indem Sie `--source-s3-presigned-url` anstelle von `--source-s3-file` verwenden. Sie müssen das `Content-Type` `headers` Feld hinzufügen. Wenn Sie beide verwenden, `InvalidParameterException` wird ein zurückgegeben.

```
--source-s3-presigned-url headers={"Name":"Value"},url=https://BUCKET.s3.REGION/
MEDIA_FILE
```

3. Verwenden Sie den send-whatsapp-messageBefehl, um die Mediennachricht zu senden.

```
aws socialmessaging send-whatsapp-message --message
 '{"messaging_product":"whatsapp","to":"'{PHONE_NUMBER}'","type":"image","image":
{"id":"'{MEDIA_ID}'"}}' --origination-phone-number-id {ORIGINATION_PHONE_NUMBER_ID}
 --meta-api-version v20.0
```

> **Note**
>
> Sie müssen die Base64-Kodierung angeben, wenn Sie AWS CLI Version 2 verwenden. Dies kann durch Hinzufügen des AWS CLI Parameters `--cli-binary-format raw-in-base64-out` oder Ändern der AWS CLI globalen Konfigurationsdatei geschehen. Weitere Informationen finden Sie `cli_binary_format`im AWS Command Line Interface User Guide für Version 2.
>
> ```
> aws socialmessaging send-whatsapp-message --message
>  '{"messaging_product":"whatsapp","to":"'{PHONE_NUMBER}'","type":"image","image":
> {"id":"'{MEDIA_ID}'"}}' --origination-phone-number-
> id {ORIGINATION_PHONE_NUMBER_ID} --meta-api-version v20.0 --cli-binary-
> format raw-in-base64-out
> ```

Gehen Sie im vorhergehenden Befehl wie folgt vor:

- *{PHONE_NUMBER}*Ersetzen Sie es durch die Telefonnummer Ihres Kunden.

- *{ORIGINATION_PHONE_NUMBER_ID}*Ersetze es durch die ID deiner Telefonnummer.
- *{MEDIA_ID}*Ersetzen Sie durch die Medien-ID, die Sie im vorherigen Schritt zurückgegeben haben.

4. Wenn Sie die Mediendatei nicht mehr benötigen, können Sie sie WhatsApp mithilfe des delete-whatsapp-message-mediaBefehls löschen. Dadurch wird nur die Mediendatei aus WhatsApp und nicht aus Ihrem Amazon S3 S3-Bucket entfernt.

```
aws socialmessaging delete-whatsapp-message-media --media-id {MEDIA_ID} --
origination-phone-number-id {ORIGINATION_PHONE_NUMBER_ID}
```

Gehen Sie im vorhergehenden Befehl wie folgt vor:

- *{ORIGINATION_PHONE_NUMBER_ID}*Ersetzen Sie es durch die ID Ihrer Telefonnummer.
- Ersetze es *{MEDIA_ID}* durch die Medien-ID.

Auf eine Nachricht in AWS End User Messaging Social antworten

Bevor Sie eine Text- oder Mediennachricht empfangen können, müssen Sie Ihr WhatsApp Geschäftskonto (WABA) und ein Veranstaltungsziel eingerichtet haben. Wenn Sie eine eingehende Nachricht erhalten, wird ein Ereignis im Amazon SNS SNS-Thema für das Ereignis gespeichert. Um eine Benachrichtigung zu erhalten, müssen Sie den Amazon SNS SNS-Themen-Endpunkt abonnieren.

Ein Beispiel für ein Ereignis im Zusammenhang mit einer empfangenen Medienmitteilung finden Sie unter WhatsApp JSON-Beispiel für den Empfang einer Mediennachricht. Weitere Informationen zur Konfiguration von finden Sie unter Configure the AWS CLI im AWS Command Line Interface Benutzerhandbuch. AWS CLI Eine Liste der unterstützten Mediendateitypen finden Sie unterUnterstützte Mediendateitypen und -größen in WhatsApp.

> **Important**
>
> Um eingehende Nachrichten empfangen zu können, müssen Sie die Ereignisziele für die WABA aktiviert haben. Weitere Informationen finden Sie unter Fügen Sie eine Nachricht und ein Ereignisziel zu AWS End User Messaging Social hinzu.

Beispiel für das Ändern des Status einer Nachricht in AWS End User Messaging Social auf „Lesen“

Sie können den Status der Nachricht so einstellen, `read` dass dem Endbenutzer zwei blaue Häkchen auf seinem Bildschirm angezeigt werden.

```
aws socialmessaging send-whatsapp-message --message
 '{"messaging_product":"whatsapp","message_id":"'{MESSAGE_ID}'","status":"read"}' --
origination-phone-number-id {ORIGINATION_PHONE_NUMBER_ID} --meta-api-version v20.0
```

Gehen Sie im vorhergehenden Befehl wie folgt vor:

- *{ORIGINATION_PHONE_NUMBER_ID}*Ersetzen Sie es durch die ID Ihrer Telefonnummer.

- *{MESSAGE_ID}*Ersetze es durch die eindeutige Kennung der Nachricht. Verwenden Sie den Wert des `id` Felds im Nachrichtenobjekt des Amazon SNS SNS-Themas.

Beispiel für die Beantwortung einer Nachricht mit einer Reaktion in AWS End User Messaging Social

Sie können der Nachricht eine Reaktion hinzufügen, z. B. einen Daumen hoch.

```
aws socialmessaging send-whatsapp-message --message
 '{"messaging_product":"whatsapp","recipient_type":"individual","to":"'{PHONE_NUMBER}'","type":
 "reaction","reaction": {"message_id": "'{MESSAGE_ID}'","emoji":"\uD83D\uDC4D"}}' --
origination-phone-number-id {ORIGINATION_PHONE_NUMBER_ID} --meta-api-version v20.0
```

Gehen Sie im vorhergehenden Befehl wie folgt vor:

- *{PHONE_NUMBER}*Ersetzen Sie es durch die Telefonnummer Ihres Kunden.
- *{MESSAGE_ID}*Ersetzen Sie es durch die eindeutige Kennung der Nachricht. Verwenden Sie den Wert des `id` Felds im Nachrichtenobjekt des Amazon SNS SNS-Themas.
- *{ORIGINATION_PHONE_NUMBER_ID}*Ersetzen Sie es durch die ID Ihrer Telefonnummer.

Laden Sie eine Mediendatei von WhatsApp zu Amazon S3 herunter

Verwenden Sie den get-whatsapp-message-mediaBefehl, um eine Mediendatei abzurufen und in einem Amazon S3 S3-Bucket zu speichern.

```
aws socialmessaging get-whatsapp-message-media --media-id {MEDIA_ID} --
origination-phone-number-id {ORIGINATION_PHONE_NUMBER_ID} --destination-s3-file
 bucketName={BUCKET},key=inbound_
{
    "mimeType": "image/jpeg",
    "fileSize": 78144
}
```

Gehen Sie im vorhergehenden Befehl wie folgt vor:

- *{BUCKET}*Ersetzen Sie durch den Namen des Amazon S3 S3-Buckets.

- *{MEDIA_ID}*Ersetzen Sie es durch den Wert des `id` Felds aus dem empfangenen Ereignis. Ein Beispiel für ein eingehendes Medienereignis finden Sie unter WhatsApp JSON-Beispiel für den Empfang einer Mediennachricht.
- *{ORIGINATION_PHONE_NUMBER_ID}*Ersetzen Sie es durch die ID Ihrer Telefonnummer.

Verwenden Sie den folgenden Befehl, um die Medien aus dem Amazon S3 S3-Bucket abzurufen:

```
aws s3 cp s3://{BUCKET}/inbound_{MEDIA_ID}.jpeg
```

Gehen Sie im vorhergehenden Befehl wie folgt vor:

- *{BUCKET}*Ersetzen Sie durch den Namen des Amazon S3 S3-Buckets.
- *{MEDIA_ID}*Ersetzen Sie es durch die MEDIA_ID, die aus dem vorherigen Schritt zurückgegeben wurde.

Beispiel für die Beantwortung einer Nachricht mit einer Lesebestätigung und einer Reaktion

In diesem Beispiel hat Ihnen Ihr Kunde Diego eine Nachricht mit „Hallo“ geschickt und Sie antworten ihm mit einer Lesebestätigung und einem Emoji mit der Hand winken.

Voraussetzungen

Um eine Benachrichtigung darüber zu erhalten, dass Diego eine Nachricht gesendet hat, müssen Sie ein Amazon SNS SNS-Thema für das Ereignis als Ziel eingerichtet und einen Themen-Endpunkt abonniert haben.

Reagieren

1. Wenn die Nachricht von Diego eingeht, wird ein Ereignis auf den Endpunkten des Themas veröffentlicht. Im Folgenden finden Sie einen Auszug dessen, was das Thema veröffentlicht.

> **Note**
>
> Da Diego die Konversation initiiert hat, wird sie nicht auf die Quote für Ihre von Ihrem Unternehmen initiierten Konversationen angerechnet.

Das ist `whatsAppWebhookEntry` in diesem Beispiel in JSON-Notation dargestellt. Ein Beispiel für die Konvertierung des `whatsAppWebhookEntry` Strings von JSON in JSON finden Sie unter WhatsApp JSON-Beispiel für den Empfang einer Nachricht.

```
{
  "context": {
    "MetaWabaIds": [
      {
        "wabaId": "1234567890abcde",
        "arn": "arn:aws:social-messaging:us-east-1:123456789012:waba/
fb2594b8a7974770b128a409e2example"
      }
    ],
    "MetaPhoneNumberIds": [
      {
        "metaPhoneNumberId": "abcde1234567890",
        "arn": "arn:aws:social-messaging:us-east-1:123456789012:phone-number-
id/976c72a700aac43eaf573ae050example"
      }
    ]
  },
  "whatsAppWebhookEntry": "{\"...JSON STRING....",
  "aws_account_id": "123456789012",
  "message_timestamp": "2025-01-08T23:30:43.271279391Z"
}
//Decoding the contents of whatsAppWebhookEntry
{
  "id": "365731266123456",
  "changes": [
    {
      "value": {
        "messaging_product": "whatsapp",
        "metadata": {
          "display_phone_number": "12065550100",
          "phone_number_id": "321010217712345"
        },
        "contacts": [
          {
            "profile": {
              "name": "Diego"
            },
```

```
            "wa_id": "12065550102"
          }
        ],
        "messages": [
          {
            "from": "14255550150",
            "id":
 "wamid.HBgLMTQyNTY5ODgzMDIVAgASGCBDNzBDRjM5MDU2ODEwMDkwREY4ODBDRDE0RjVGRkexample",
            "timestamp": "1723506035",
            "text": {
              "body": "Hi"
            },
            "type": "text"
          }
        ]
      },
      "field": "messages"
    }
  ]
}
```

2. Um Diego zu zeigen, dass Sie die Nachricht erhalten haben, setzen Sie den Status auf`read`. Diego sieht zwei blaue Häkchen neben der Nachricht auf seinem Gerät.

> **Note**
>
> Sie müssen die Base64-Kodierung angeben, wenn Sie AWS CLI Version 2 verwenden. Dies kann durch Hinzufügen des AWS CLI Parameters `--cli-binary-format raw-in-base64-out` oder Ändern der AWS CLI globalen Konfigurationsdatei geschehen. Weitere Informationen finden Sie `cli_binary_format`im AWS Command Line Interface User Guide für Version 2.

```
aws socialmessaging send-whatsapp-message --message
 '{"messaging_product":"whatsapp","message_id":"'{MESSAGE_ID}'","status":"read"}'
 --origination-phone-number-id {ORIGINATION_PHONE_NUMBER_ID} --meta-api-version
 v20.0
```

Gehen Sie im vorhergehenden Befehl wie folgt vor:

- *{ORIGINATION_PHONE_NUMBER_ID}*Ersetzen Sie es durch die Telefonnummer, an die Diego seine Nachricht gesendet hatphone-number-id-976c72a700aac43eaf573ae050example.
- *{MESSAGE_ID}*Ersetzen Sie es durch die eindeutige Kennung der Nachricht. Dies ist derselbe Wert wie das id Feld in der empfangenen Nachrichtwamid.HBgLMTQyNTY5ODgzMDIVAgASGCBDNzBDRjM5MDU2ODEwMDkwREY4ODBDRDE0Rj

3. Du kannst Diego eine Handwinkenreaktion schicken.

```
aws socialmessaging send-whatsapp-message --message
 '{"messaging_product":"whatsapp","recipient_type":"individual","to":"'{PHONE_NUMBER}'","ty
 "reaction","reaction": {"message_id": "'{MESSAGE_ID}'","emoji":"\uD83D\uDC4B"}}'
 --origination-phone-number-id {ORIGINATION_PHONE_NUMBER_ID} --meta-api-version
 v20.0
```

Gehen Sie im vorhergehenden Befehl wie folgt vor:

- *{PHONE_NUMBER}*Ersetze es durch Diegos Telefonnummer,14255550150.
- *{MESSAGE_ID}*Ersetze es durch die eindeutige Kennung der Nachricht. Dies ist derselbe Wert wie das id Feld in der empfangenen Nachrichtwamid.HBgLMTQyNTY5ODgzMDIVAgASGCBDNzBDRjM5MDU2ODEwMDkwREY4ODBDRDE0Rj
- *{ORIGINATION_PHONE_NUMBER_ID}*Ersetzen Sie durch die Telefonnummer, an die Diego seine Nachricht gesendet hat:phone-number-id-976c72a700aac43eaf573ae050example.

Weitere Ressourcen

- Aktivieren Sie Ereignisziele, um Ereignisse zu protokollieren und eingehende Nachrichten zu empfangen.
- Eine Liste der WhatsApp Nachrichtenobjekte finden Sie unter Nachrichten in der WhatsApp Business Platform Cloud API-Referenz.

Grundlegendes zu WhatsApp Abrechnungs- und Nutzungsberichten für AWS End User Messaging Social

Es gibt zwei Arten von WhatsApp Abrechnungs- und Nutzungsberichten für AWS End User Messaging Social:

- Wird pro Konversation berechnet
- Wird pro Nachricht berechnet

Weitere Informationen zu diesen Abrechnungs- und Berichtstypen finden Sie in den folgenden Themen.

Themen

Wird pro Konversation berechnet

> **Note**
>
> Ab dem 1. Juli 2025 berechnet AWS End User Messaging Social entsprechend der Änderung von Meta pro Nachricht statt pro Konversation Gebühren für WhatsApp Nachrichten. Das bedeutet, dass Ihnen `MetaTemplateMessageFee` statt der `ConversationFee` Meta-Gebühr eine Gebühr berechnet wird, zusätzlich zu den AWS `MessageFee`. Diese Änderungen sind in Ihren monatlichen Rechnungen enthalten, beginnend mit der Rechnung für Juli 2025, die Sie im August 2025 erhalten. Informationen zu Abrechnungs- und Nutzungsberichten, wenn Ihnen eine Rechnung pro Nachricht berechnet wird, finden Sie unterthe section called “Wird pro Nachricht abgerechnet”.

Der Social Channel AWS End User Messaging generiert einen Nutzungstyp, der fünf Felder im folgenden Format enthält:*`Region code`*`-`*`MessagingType`*`-`*`ISO`*`-`*`FeeDescription`*`-`*`FeeType`*. Für jede WhatsApp Konversation gibt es zwei mögliche Abrechnungsposten WhatsApp`ConversationFee`, die, und die AWS pro`MessageFee`.

Wenn Sie eine Konversation initiieren, indem Sie eine Vorlagennachricht senden, werden Ihnen eine WhatsApp `ConversationFee` und eine AWS pro `MessageFee` Nachricht in Rechnung gestellt. Dadurch wird ein 24-Stunden-Fenster geöffnet, in dem jede Nachricht, die Sie von demselben Kunden senden oder empfangen, als Pers abgerechnet wird. AWS `MessageFee`

Die Art der WhatsApp Konversation und die Preisdetails finden Sie unter Konversationsbasierte Preisgestaltung im WhatsApp Business Platform Developer Guide.

In der folgenden Tabelle werden die möglichen Werte und Beschreibungen für die Felder im Nutzungstyp angezeigt. Weitere Informationen zu den Preisen für AWS End User Messaging Social finden Sie unter WhatsAppPreise für AWS End User Messaging.

Feld	Optionen	Beschreibung
`Region code`	• USE1— Region USA Ost (Nord-Virginia) • USE2— Region USA Ost (Ohio) • USW2— Region USA West (Oregon) • APS3— Region Asien-Paz ifik (Mumbai) • APS5— Region Asien-Paz ifik (Hyderabad) • APS1— Region Asien-Paz ifik (Singapur) • APS2— Region Asien-Paz ifik (Sydney) • EU – Region Europa (Irland) • EUW2— Region Europa (London) • APN1— Region Asien-Paz ifik (Tokio) • APN2— Region Asien-Paz ifik (Seoul)	Das AWS-Region Präfix, das angibt, von wo die WhatsApp Nachricht gesendet oder empfangen wurde.

Feld	Optionen	Beschreibung
	• EUC1— Region Europa (Frankfurt) • EUS2— Region Europa (Spanien) • SAE1— Region Südamerika (São Paulo) • AFS1— Region Afrika (Kapstadt) • CAN1— Region Kanada (Zentral)	
MessagingType	`WhatsApp`	Dieses Feld identifiziert den Typ der gesendeten Nachricht.
ISO	Siehe unterstützte Länder	Der zweistellige ISO-Ländercode, an den die Nachricht gesendet wurde.
FeeDescription	`ConversationFee` , `MessageFee`	Dieses Feld gibt entweder den WhatsApp `ConversationFee` oder den AWS pro an`MessageFee` .

Feld	Optionen	Beschreibung
FeeType	`Authentication` , `Authentication-International` , `Marketing` , `Service`, `Utility`, `Standard`	In diesem Feld wird angezeigt , welche Art von Konversation verwendet wurde, oder es gibt die Standardgebühr pro Nachricht an Vom Unternehmen initiierte **`ConversationFee`** Kategorien • `Marketing` — Wird verwendet, um eine Vielzahl von Zielen zu erreichen , von der Steigerung des Bekanntheitsgrades über die Steigerung des Umsatzes bis hin zur Retargeting von Kunden. Beispiele hierfür sind Ankündigungen neuer Produkte, Dienstleistungen oder Funktionen, gezielte Werbeaktionen/Angebote und Erinnerungen an abgebrochene Einkaufswagen. • `Utility`— Wird verwendet , um Benutzeraktionen oder Anfragen nachzuverfolgen. Beispiele hierfür sind die Bestätigung, order/delivery Verwaltung (z. B. ein Lieferupdate), Kontoaktualisierungen oder Benachrichtigungen (z. B.

Feld	Optionen	Beschreibung
		eine Zahlungserinnerung) oder Feedback-Umfragen. • `Authentication` — Wird verwendet, um Benutzer mit Einmalpasswörtern zu authentifizieren, möglicher weise in mehreren Schritten des Anmeldevorgangs (z. B. Kontoverifizierung, Kontowiederherstellung und Integritätsprobleme). • `Authentication-International` — Wird genauso verwendet wie, `Authentication` aber Ihr Unternehmen hat Anspruch auf die Tarife von Authentication International, hat seinen Sitz in einem anderen Land und die Konversation wurde an oder nach der Startzeit für das Land eröffnet. • `Service`— Wird zur Lösung von Kundenanf ragen verwendet. Vom Benutzer initiierte **`ConversationFee`** Kategorien • `Service`— Wird zur Lösung von Kundenanf ragen verwendet.

Feld	Optionen	Beschreibung
		`MessageFee` -Kategorien • `Standard`— Gebühr pro gesendeter oder empfangener Nachricht.

Wenn Sie eine Konversation initiieren, indem Sie eine Vorlagennachricht senden, werden Ihnen eins `ConversationFee` und eins `MessageFee` in Rechnung gestellt. Dadurch wird ein 24-Stunden-Fenster geöffnet, in dem jede Vorlagennachricht, die Sie an denselben Kunden senden, einzeln in Rechnung gestellt wird. `MessageFee` Während des 24-Stunden-Fensters müssen die Vorlagennachrichten vom gleichen Typ sein, sonst wird eine neue Konversation gestartet.

Wenn Sie beispielsweise eine Marketing-Vorlagennachricht an einen Kunden senden, wird Ihnen das `ConversationFee` und `MessageFee` in Rechnung gestellt.

```
Marketing Template Message 1: APS1-WhatsApp-CA-ConversationFee-Marketing
Marketing Template Message 1: APS1-WhatsApp-CA-MessageFee-Standard
Marketing Template Message 2: APS1-WhatsApp-CA-MessageFee-Standard
```

Wenn der Kunde Ihnen eine Nachricht sendet und Sie darauf antworten, wird Ihnen das Öffnen einer neuen `Service` Konversation und Nachricht in Rechnung gestellt.

```
Service Message 1: APS1-WhatsApp-CA-ConversationFee-Service
Service Message 1: APS1-WhatsApp-CA-MessageFee-Standard
Service Message 2: APS1-WhatsApp-CA-MessageFee-Standard
Service Message 3: APS1-WhatsApp-CA-MessageFee-Standard
```

Wann gilt das Authentication-International FeeType

Eine Liste der Länder mit einem `Authentication-International` FeeType finden Sie unter Preise für WhatsApp AWS Endbenutzer-Messaging.

Wenn Sie eine `Authentication` Konversation mit einem WhatsApp Nutzer eröffnen, dessen Landesvorwahl eine hat `Authentication-International` FeeType, wird Ihnen in folgenden Fällen der `Authentication-International` Tarif für dieses Land in Rechnung gestellt:

1. Ihr Unternehmen eröffnet innerhalb von 30 Tagen mehr als 750.000 Konversationen über alle Ihre WhatsApp Geschäftskonten mit WhatsApp Nutzern, deren Landesvorwahlen für ein Land gelten, für das es einen Tarif gibt. `Authentication-International` Weitere Informationen finden Sie unter Eignung im WhatsApp Business Platform Developer Guide.

   > **Important**
   >
   > Wenn Meta feststellt, dass Ihr Unternehmen dafür in Frage kommt, `Authentication-International` wird es versuchen, Ihnen eine E-Mail-Benachrichtigung mit den entsprechenden Ländern und den neuen Startzeiten für den Zeitraum von 30 Tagen zu senden.

2. Ihr Unternehmen hat seinen Sitz in einem anderen Land. Weitere Informationen zur Verwaltung des Standorts Ihres Unternehmens finden Sie unter Hauptgeschäftsstandort im WhatsApp Business Platform Developer Guide.
3. Die Konversation wurde an oder nach Ihrer Startzeit für dieses Land eröffnet

Beispiel 1: Senden einer Marketing-Vorlagennachricht

Wenn Sie beispielsweise eine Marketing-Vorlagennachricht an einen Kunden senden, wird Ihnen eine Nachricht WhatsApp `ConversationFee` und eine AWS pro `MessageFee` Nachricht in Rechnung gestellt.

```
Marketing Template Message 1: APS1-WhatsApp-CA-ConversationFee-Marketing
Marketing Template Message 1: APS1-WhatsApp-CA-MessageFee-Standard
```

Beispiel 2: Öffnen einer Servicegespräche

Eine Servicegebühr fällt an, wenn ein Unternehmen auf eine eingehende Nachricht eines Benutzers reagiert, die außerhalb eines aktiven 24-Stunden-Gesprächsfensters liegt, das vom Unternehmen initiiert wurde. In diesem Szenario werden Ihnen AWS `MessageFee` für jede eingehende und ausgehende WhatsApp `ConversationFee` Nachricht eine und eine in Rechnung gestellt.

```
Service Message 1: APS1-WhatsApp-CA-ConversationFee-Service
Service Message 1: APS1-WhatsApp-CA-MessageFee-Standard
Service Message 2: APS1-WhatsApp-CA-MessageFee-Standard
Service Message 3: APS1-WhatsApp-CA-MessageFee-Standard
```

AWS ISO-Codes für Rechnungsstellung an Endbenutzer und WhatsApp Zuordnung von Gesprächsgebühren in sozialen Netzwerken

Unterstützte Länder

Zweistelliger ISO-Ländercode	Ländername	WhatsApp Region für die Abrechnung der Konversation
AF	Afghanistan	Rest of Asia Pacific
AX	Aland Islands	Other
AL	Albania	Rest of Central & Eastern Europe
DZ	Algeria	Rest of Africa
AS	American Samoa	Other
AD	Andorra	Other
AO	Angola	Rest of Africa
AI	Anguilla	Other
AQ	Antarctica	Other
AG	Antigua and Barbuda	Other
AR	Argentina	Argentina
AM	Armenia	Rest of Central & Eastern Europe
AW	Aruba	Other
AC	Ascension Island	Other
AU	Australia	Rest of Asia Pacific
AT	Austria	Rest of Western Europe

Zweistelliger ISO-Ländercode	Ländername	WhatsApp Region für die Abrechnung der Konversation
AZ	Azerbaijan	Rest of Central & Eastern Europe
BS	Bahamas	Other
BH	Bahrain	Rest of Middle East
BD	Bangladesh	Rest of Asia Pacific
BB	Barbados	Other
BY	Belarus	Rest of Central & Eastern Europe
BE	Belgium	Rest of Western Europe
BZ	Belize	Other
BJ	Benin	Rest of Africa
BM	Bermuda	Other
BT	Bhutan	Other
BO	Bolivia	Rest of Latin America
BQ	Bonaire	Other
BA	Bosnia and Herzegovina	Other
BW	Botswana	Rest of Africa
BV	Bouvet Island	Other
BR	Brazil	Brazil
IO	British Indian Ocean Territory	Other
VG	British Virgin Islands	Other

Zweistelliger ISO-Ländercode	Ländername	WhatsApp Region für die Abrechnung der Konversation
BN	Brunei Darussalam	Other
BG	Bulgaria	Rest of Central & Eastern Europe
BF	BurkinaFaso	Rest of Africa
BI	Burundi	Rest of Africa
KH	Cambodia	Rest of Asia Pacific
CM	Cameroon	Rest of Africa
CA	Canada	North America
CV	Cape Verde	Other
KY	Cayman Islands	Other
CF	Central African Republic	Other
TD	Chad	Rest of Africa
CL	Chile	Chile
CN	China	Rest of Asia Pacific
CX	Christmas Island	Other
CC	Cocos(Keeling) Islands	Other
CO	Colombia	Colombia
KM	Comoros	Other
CK	Cook Islands	Other
CR	Costa Rica	Rest of Latin America

Zweistelliger ISO-Ländercode	Ländername	WhatsApp Region für die Abrechnung der Konversation
CI	Cote d'Ivoire	Rest of Africa
HR	Croatia	Rest of Central & Eastern Europe
CW	Curacao	Other
CY	Cyprus	Other
CZ	Czech Republic	Rest of Central & Eastern Europe
CD	Democratic Republic of the Congo	Rest of Africa
DK	Denmark	Rest of Western Europe
DJ	Djibouti	Other
DM	Dominica	Other
DO	Dominican Republic	Rest of Latin America
EC	Ecuador	Rest of Latin America
EG	Egypt	Egypt
SV	El Salvador	Rest of Latin America
GQ	Equatorial Guinea	Other
ER	Eritrea	Rest of Africa
EE	Estonia	Other
ET	Ethiopia	Rest of Africa
SZ	Eswatini	Rest of Africa

Zweistelliger ISO-Ländercode	Ländername	WhatsApp Region für die Abrechnung der Konversation
FK	Falkland Islands	Other
FO	Faroe Islands	Other
FJ	Fiji	Other
FI	Finland	Rest of Western Europe
FR	France	France
GF	French Guiana	Other
PF	French Polynesia	Other
TF	French Southern Territories	Other
GA	Gabon	Rest of Africa
GM	Gambia	Rest of Africa
GE	Georgia	Rest of Central & Eastern Europe
DE	Germany	Germany
GH	Ghana	Rest of Africa
GI	Gibraltar	Other
GR	Greece	Rest of Central & Eastern Europe
GL	Greenland	Other
GD	Grenada	Other
GP	Guadeloupe	Other
GU	Guam	Other

Zweistelliger ISO-Ländercode	Ländername	WhatsApp Region für die Abrechnung der Konversation
GT	Guatemala	Rest of Latin America
GG	Guernsey	Other
GN	Guinea	Other
GW	Guinea-Bissau	Rest of Africa
GY	Guyana	Other
HT	Haiti	Rest of Latin America
HM	Heard and McDonald Islands	Other
HN	Honduras	Rest of Latin America
HK	Hong Kong	Rest of Asia Pacific
HU	Hungary	Rest of Central & Eastern Europe
IS	Iceland	Other
IN	India	India
ID	Indonesia	Indonesia
IQ	Iraq	Rest of Middle East
IE	Ireland	Rest of Western Europe
IM	Isle of Man	Other
IL	Israel	Israel
IT	Italy	Italy
JM	Jamaica	Rest of Latin America

Zweistelliger ISO-Ländercode	Ländername	WhatsApp Region für die Abrechnung der Konversation
JP	Japan	Rest of Asia Pacific
JE	Jersey	Other
JO	Jordan	Rest of Middle East
KZ	Kazakhstan	Other
KE	Kenya	Rest of Africa
KI	Kiribati	Other
XK	Kosovo	Other
KW	Kuwait	Rest of Middle East
KG	Kyrgyzstan	Other
LA	Lao PDR	Rest of Asia Pacific
LV	Latvia	Rest of Central & Eastern Europe
LB	Lebanon	Rest of Middle East
LS	Lesotho	Rest of Africa
LR	Liberia	Rest of Africa
LY	Libya	Rest of Africa
LI	Liechtenstein	Other
LT	Lithuania	Rest of Central & Eastern Europe
LU	Luxembourg	Other
MO	Macao	Other

Zweistelliger ISO-Ländercode	Ländername	WhatsApp Region für die Abrechnung der Konversation
MK	Macedonia	Rest of Central & Eastern Europe
MG	Madagascar	Rest of Africa
MW	Malawi	Rest of Africa
MY	Malaysia	Malaysia
MV	Maldives	Other
ML	Mali	Rest of Africa
MT	Malta	Other
MH	Marshall Islands	Other
MQ	Martinique	Other
MR	Mauritania	Rest of Africa
MU	Mauritius	Other
YT	Mayotte	Other
MX	Mexico	Mexico
FM	Micronesia	Other
MD	Moldova	Rest of Central & Eastern Europe
MC	Monaco	Other
MN	Mongolia	Rest of Asia Pacific
ME	Montenegro	Other
MS	Montserrat	Other

Zweistelliger ISO-Ländercode	Ländername	WhatsApp Region für die Abrechnung der Konversation
MA	Morocco	Rest of Africa
MZ	Mozambique	Rest of Africa
MM	Myanmar	Other
NA	Namibia	Rest of Africa
NR	Nauru	Other
NP	Nepal	Rest of Asia Pacific
NL	Netherlands	Netherlands
NC	New Caledonia	Other
NZ	New Zealand	Rest of Asia Pacific
NI	Nicaragua	Rest of Latin America
NE	Niger	Rest of Africa
NG	Nigeria	Nigeria
NU	Niue	Other
NF	Norfolk Island	Other
MP	Northern Mariana Islands	Other
NO	Norway	Rest of Western Europe
OM	Oman	Rest of Middle East
PK	Pakistan	Pakistan
PW	Palau	Other
PS	Palestinian Territory	Other

Zweistelliger ISO-Ländercode	Ländername	WhatsApp Region für die Abrechnung der Konversation
PA	Panama	Rest of Latin America
PG	Papua New Guinea	Rest of Asia Pacific
PY	Paraguay	Rest of Latin America
PE	Peru	Peru
PH	Philippines	Rest of Asia Pacific
PN	Pitcairn	Other
PL	Poland	Rest of Central & Eastern Europe
PT	Portugal	Rest of Western Europe
PR	Puerto Rico	Rest of Latin America
QA	Qatar	Rest of Middle East
CG	Republic of Congo	Other
RE	Reunion	Other
RO	Romania	Rest of Central & Eastern Europe
RU	Russian Federation	Russia
RW	Rwanda	Rest of Africa
SH	Saint Helena	Other
KN	Saint Kitts and Nevis	Other
LC	Saint Lucia	Other
PM	Saint Pierre and Miquelon	Other

Zweistelliger ISO-Ländercode	Ländername	WhatsApp Region für die Abrechnung der Konversation
VC	Saint Vincent and Grenadines	Other
BL	Saint-Barthelemy	Other
MF	Saint-Martin	Other
WS	Samoa	Other
SM	San Marino	Other
ST	Sao Tome and Principe	Other
SA	Saudi Arabia	Saudi Arabia
SN	Senegal	Rest of Africa
RS	Serbia	Rest of Central & Eastern Europe
SC	Seychelles	Other
SL	Sierra Leone	Rest of Africa
SG	Singapore	Rest of Asia Pacific
SX	Sint Maarten	Other
SK	Slovakia	Rest of Central & Eastern Europe
SI	Slovenia	Rest of Central & Eastern Europe
SB	Solomon Islands	Other
SO	Somalia	Rest of Africa
ZA	South Africa	South Africa

Zweistelliger ISO-Ländercode	Ländername	WhatsApp Region für die Abrechnung der Konversation
GS	South Georgia and the South Sandwich Islands	Other
KR	South Korea	Other
SS	South Sudan	Rest of Africa
ES	Spain	Spain
LK	Sri Lanka	Rest of Asia Pacific
SR	Suriname	Other
SJ	Svalbard and Jan Mayen Islands	Other
SE	Sweden	Rest of Western Europe
CH	Switzerland	Rest of Western Europe
TW	Taiwan	Rest of Asia Pacific
TJ	Tajikistan	Rest of Asia Pacific
TZ	Tanzania	Rest of Africa
TH	Thailand	Rest of Asia Pacific
TL	Timor-Leste	Other
TG	Togo	Rest of Africa
TK	Tokelau	Other
TO	Tonga	Other
TT	Trinidad and Tobago	Other
TA	Tristan da Cunha	Other

Zweistelliger ISO-Ländercode	Ländername	WhatsApp Region für die Abrechnung der Konversation
TN	Tunisia	Rest of Africa
TR	Turkey	Turkey
TM	Turkmenistan	Rest of Asia Pacific
TC	Turks and Caicos Islands	Other
TV	Tuvalu	Other
UG	Uganda	Rest of Africa
UA	Ukraine	Rest of Central & Eastern Europe
AE	United Arab Emirates	United Arab Emirates
GB	United Kingdom	United Kingdom
US	United States	North America
UY	Uruguay	Rest of Latin America
UM	US Minor Outlying Islands	Other
UZ	Uzbekistan	Rest of Asia Pacific
VU	Vanuatu	Other
VA	Vatican City State	Other
VE	Venezuela	Rest of Latin America
VN	Vietnam	Rest of Asia Pacific
VI	Virgin Islands	Other
WF	Wallis and Futuna Islands	Other

Zweistelliger ISO-Ländercode	Ländername	WhatsApp Region für die Abrechnung der Konversation
EH	Western Sahara	Other
YE	Yemen	Rest of Middle East
ZM	Zambia	Rest of Africa
ZW	Zimbabwe	Other

Wird pro Nachricht abgerechnet

> **Note**
>
> Ab dem 1. Juli 2025 berechnet AWS End User Messaging Social entsprechend der Änderung von Meta pro Nachricht statt pro Konversation Gebühren für WhatsApp Nachrichten. Das bedeutet, dass Ihnen `MetaTemplateMessageFee` statt der `ConversationFee` Meta-Gebühr eine Gebühr berechnet wird, zusätzlich zu den AWS `MessageFee`. Diese Änderungen sind in Ihren monatlichen Rechnungen enthalten, beginnend mit der Rechnung für Juli 2025, die Sie im August 2025 erhalten. Informationen zu früheren Rechnungen, die auf basieren`ConversationFee`, finden Sie unterthe section called “Wird pro Konversation berechnet”.

Der Social Channel AWS End User Messaging generiert einen Nutzungstyp, der fünf Felder im folgenden Format enthält:*`Region code`*`-`*`MessagingType`*`-`*`ISO`*`-`*`FeeDescription`*`-`*`FeeType`*. Für jede WhatsApp Nachricht gibt es zwei mögliche Abrechnungsposten: die`MetaTemplateMessageFee`, und die AWS `MessageFee`.

Wenn Sie eine Vorlagennachricht senden, werden Ihnen eine WhatsApp `MetaTemplateMessageFee` und eine AWS pro `MessageFee` Nachricht in Rechnung gestellt.

In der folgenden Tabelle werden die möglichen Werte und Beschreibungen für die Felder im Nutzungstyp angezeigt. Weitere Informationen zu den Preisen für AWS End User Messaging Social finden Sie unter WhatsAppPreise für AWS End User Messaging.

Feld	Optionen	Beschreibung
Region code	• USE1— Region USA Ost (Nord-Virginia) • USE2— Region USA Ost (Ohio) • USW2— Region USA West (Oregon) • APS3— Region Asien-Pazifik (Mumbai) • APS5— Region Asien-Pazifik (Hyderabad) • APS1— Region Asien-Pazifik (Singapur) • APS2— Region Asien-Pazifik (Sydney) • EU – Region Europa (Irland) • EUW2— Region Europa (London) • APN1— Region Asien-Pazifik (Tokio) • APN2— Region Asien-Pazifik (Seoul) • EUC1— Region Europa (Frankfurt) • EUS2— Region Europa (Spanien) • SAE1— Region Südamerika (São Paulo) • AFS1— Region Afrika (Kapstadt) • CAN1— Region Kanada (Zentral)	Das AWS-Region Präfix, das angibt, von wo die WhatsApp Nachricht gesendet oder empfangen wurde.

Feld	Optionen	Beschreibung
MessagingType	WhatsApp	Dieses Feld identifiziert den Typ der gesendeten Nachricht.
ISO	Siehe unterstützte Länder	Der zweistellige ISO-Ländercode, an den die Nachricht gesendet wurde.
FeeDescription	MetaTemplateMessageFee , MessageFee	Dieses Feld gibt entweder den WhatsApp MetaTemplateMessageFee oder den AWS proanMessageFee .

Feld	Optionen	Beschreibung
FeeType	`Authentication` , `Authentication-International` , `Marketing` , `Service`, `Utility`, `Standard`	In diesem Feld wird der Typ der verwendeten Nachricht angezeigt oder die Standardgebühr pro Nachricht angegeben Vom Unternehmen initiierte **`MetaTemplateMessageFee`** Kategorien • `Marketing` — Wird verwendet, um eine Vielzahl von Zielen zu erreichen, von der Steigerung des Bekanntheitsgrades über die Steigerung des Umsatzes bis hin zur Retargeting von Kunden. Beispiele hierfür sind Ankündigungen neuer Produkte, Dienstleistungen oder Funktionen, gezielte Werbeaktionen/Angebote und Erinnerungen an abgebrochene Einkaufswagen. • `Utility`— Wird verwendet, um Benutzeraktionen oder Anfragen nachzuverfolgen. Beispiele hierfür sind die Bestätigung, order/delivery Verwaltung (z. B. ein Lieferupd

Feld	Optionen	Beschreibung
		ate), Kontoaktualisierungen oder Benachrichtigungen (z. B. eine Zahlungserinnerung) oder Feedback-Umfragen. • `Authentication` — Wird verwendet, um Benutzer mit Einmalpasswörtern zu authentifizieren, möglicherweise in mehreren Schritten des Anmeldevorgangs (z. B. Kontoverifizierung, Kontowiederherstellung und Integritätsprobleme). • `Authentication-International` — Wird genauso verwendet wie, `Authentication` aber Ihr Unternehmen hat Anspruch auf die Tarife von Authentication International, hat seinen Sitz in einem anderen Land, und die Nachricht wurde an oder nach der Startzeit für das Land gesendet. • `Service`— Wird zur Lösung von Kundenanfragen verwendet.

Feld	Optionen	Beschreibung
		Vom Benutzer initiierte **`MetaTemplateMessageFee`** Kategorien • `Service`— Wird zur Lösung von Kundenanfragen verwendet. **`MessageFee`** -Kategorien • `Standard`— Gebühr pro gesendeter oder empfangener Nachricht.

Wenn Sie eine Vorlagennachricht senden, werden Ihnen eins `MetaTemplateMessageFee` und eins `MessageFee` in Rechnung gestellt. Wenn Sie Textnachrichten in freier Form senden oder eingehende Nachrichten empfangen, wird Ihnen der in Rechnung gestellt. `MessageFee`

Wenn Sie beispielsweise eine Marketing-Vorlagennachricht an einen Kunden senden, wird Ihnen das und in Rechnung gestellt. `MetaTemplateMessageFee` `MessageFee`

Wann gilt das Authentication-International FeeType

Eine Liste der Länder mit einem `Authentication-International` FeeType finden Sie unter Preise für WhatsApp AWS Endbenutzer-Messaging.

Wenn Sie eine `Authentication` Nachricht an einen WhatsApp Nutzer senden, dessen Landesvorwahl eine hat `Authentication-International` FeeType, wird Ihnen in folgenden Fällen der `Authentication-International` Tarif für dieses Land in Rechnung gestellt:

1. Ihr Unternehmen öffnet innerhalb von 30 Tagen mehr als 750.000 Nachrichten für alle Ihre WhatsApp Geschäftskonten mit WhatsApp Nutzern, deren Landesvorwahlen für ein Land gelten, für das es einen Tarif gibt. `Authentication-International` Weitere Informationen finden Sie unter Eignung im WhatsApp Business Platform Developer Guide.

> **Important**
>
> Wenn Meta feststellt, dass Ihr Unternehmen dafür in Frage kommt, `Authentication-International` wird es versuchen, Ihnen eine E-Mail-Benachrichtigung mit den entsprechenden Ländern und den neuen Startzeiten für den Zeitraum von 30 Tagen zu senden.

2. Ihr Unternehmen hat seinen Sitz in einem anderen Land. Weitere Informationen zur Verwaltung des Standorts Ihres Unternehmens finden Sie unter Hauptgeschäftsstandort im WhatsApp Business Platform Developer Guide.
3. Die Nachricht wurde an oder nach Ihrer Startzeit des 30-Tage-Zeitraums für dieses Land gesendet.

Beispiel 1: Senden einer Marketing-Vorlagennachricht

Wenn Sie beispielsweise eine Marketing-Vorlagennachricht an einen Kunden senden, wird Ihnen eine Nachricht WhatsApp `MetaTemplateMessageFee` und eine AWS pro `MessageFee` Nachricht in Rechnung gestellt.

```
Marketing Template Message 1: APS1-WhatsApp-CA-MetaTemplateMessageFee-Marketing_Regular
Marketing Template Message 1: APS1-WhatsApp-CA-MessageFee-Standard
```

Beispiel 2: Öffnen einer Servicegespräche

Eine Servicekonversation entsteht, wenn ein Unternehmen innerhalb von 24 Stunden nach Erhalt der vom Benutzer initiierten Nachricht auf die eingehende Nachricht eines Benutzers reagiert. In diesem Szenario werden Ihnen eine Gebühr und AWS `MessageFee` für jede eingehende und ausgehende Nachricht eine `MetaTemplateMessageFee-Service_Regular` Gebühr in Rechnung gestellt. Wenn beispielsweise ein Benutzer eine Nachricht initiiert hat, das Unternehmen darauf geantwortet hat und der Benutzer geantwortet hat, wären die Gebühren für die drei Nachrichten wie folgt:

```
User Initiated Message 1: APS1-WhatsApp-CA-MessageFee-StandardService
Business Initiated Message 2: APS1-WhatsApp-CA-MetaTemplateMessageFee-Service_Regular
Business Initiated Message 2: APS1-WhatsApp-CA-MessageFee-StandardService
User Initiated Message 3: APS1-WhatsApp-CA-MessageFee-StandardService
```

AWS Endbenutzer-Nachrichten, soziale Netzwerke, Abrechnung, ISO-Codes und MetaTemplateMessageFee Zuordnung

Unterstützte Länder

Zweistelliger ISO-Ländercode	Ländername	WhatsApp Region für die Abrechnung der Konversation
AF	Afghanistan	Rest of Asia Pacific
AX	Aland Islands	Other
AL	Albania	Rest of Central & Eastern Europe
DZ	Algeria	Rest of Africa
AS	American Samoa	Other
AD	Andorra	Other
AO	Angola	Rest of Africa
AI	Anguilla	Other
AQ	Antarctica	Other
AG	Antigua and Barbuda	Other
AR	Argentina	Argentina
AM	Armenia	Rest of Central & Eastern Europe
AW	Aruba	Other
AC	Ascension Island	Other
AU	Australia	Rest of Asia Pacific
AT	Austria	Rest of Western Europe

Zweistelliger ISO-Ländercode	Ländername	WhatsApp Region für die Abrechnung der Konversation
AZ	Azerbaijan	Rest of Central & Eastern Europe
BS	Bahamas	Other
BH	Bahrain	Rest of Middle East
BD	Bangladesh	Rest of Asia Pacific
BB	Barbados	Other
BY	Belarus	Rest of Central & Eastern Europe
BE	Belgium	Rest of Western Europe
BZ	Belize	Other
BJ	Benin	Rest of Africa
BM	Bermuda	Other
BT	Bhutan	Other
BO	Bolivia	Rest of Latin America
BQ	Bonaire	Other
BA	Bosnia and Herzegovina	Other
BW	Botswana	Rest of Africa
BV	Bouvet Island	Other
BR	Brazil	Brazil
IO	British Indian Ocean Territory	Other
VG	British Virgin Islands	Other

Zweistelliger ISO-Ländercode	Ländername	WhatsApp Region für die Abrechnung der Konversation
BN	Brunei Darussalam	Other
BG	Bulgaria	Rest of Central & Eastern Europe
BF	BurkinaFaso	Rest of Africa
BI	Burundi	Rest of Africa
KH	Cambodia	Rest of Asia Pacific
CM	Cameroon	Rest of Africa
CA	Canada	North America
CV	Cape Verde	Other
KY	Cayman Islands	Other
CF	Central African Republic	Other
TD	Chad	Rest of Africa
CL	Chile	Chile
CN	China	Rest of Asia Pacific
CX	Christmas Island	Other
CC	Cocos(Keeling) Islands	Other
CO	Colombia	Colombia
KM	Comoros	Other
CK	Cook Islands	Other
CR	Costa Rica	Rest of Latin America

Zweistelliger ISO-Ländercode	Ländername	WhatsApp Region für die Abrechnung der Konversation
CI	Cote d'Ivoire	Rest of Africa
HR	Croatia	Rest of Central & Eastern Europe
CW	Curacao	Other
CY	Cyprus	Other
CZ	Czech Republic	Rest of Central & Eastern Europe
CD	Democratic Republic of the Congo	Rest of Africa
DK	Denmark	Rest of Western Europe
DJ	Djibouti	Other
DM	Dominica	Other
DO	Dominican Republic	Rest of Latin America
EC	Ecuador	Rest of Latin America
EG	Egypt	Egypt
SV	El Salvador	Rest of Latin America
GQ	Equatorial Guinea	Other
ER	Eritrea	Rest of Africa
EE	Estonia	Other
ET	Ethiopia	Rest of Africa
SZ	Eswatini	Rest of Africa

Zweistelliger ISO-Ländercode	Ländername	WhatsApp Region für die Abrechnung der Konversation
FK	Falkland Islands	Other
FO	Faroe Islands	Other
FJ	Fiji	Other
FI	Finland	Rest of Western Europe
FR	France	France
GF	French Guiana	Other
PF	French Polynesia	Other
TF	French Southern Territories	Other
GA	Gabon	Rest of Africa
GM	Gambia	Rest of Africa
GE	Georgia	Rest of Central & Eastern Europe
DE	Germany	Germany
GH	Ghana	Rest of Africa
GI	Gibraltar	Other
GR	Greece	Rest of Central & Eastern Europe
GL	Greenland	Other
GD	Grenada	Other
GP	Guadeloupe	Other
GU	Guam	Other

Zweistelliger ISO-Ländercode	Ländername	WhatsApp Region für die Abrechnung der Konversation
GT	Guatemala	Rest of Latin America
GG	Guernsey	Other
GN	Guinea	Other
GW	Guinea-Bissau	Rest of Africa
GY	Guyana	Other
HT	Haiti	Rest of Latin America
HM	Heard and McDonald Islands	Other
HN	Honduras	Rest of Latin America
HK	Hong Kong	Rest of Asia Pacific
HU	Hungary	Rest of Central & Eastern Europe
IS	Iceland	Other
IN	India	India
ID	Indonesia	Indonesia
IQ	Iraq	Rest of Middle East
IE	Ireland	Rest of Western Europe
IM	Isle of Man	Other
IL	Israel	Israel
IT	Italy	Italy
JM	Jamaica	Rest of Latin America

Zweistelliger ISO-Ländercode	Ländername	WhatsApp Region für die Abrechnung der Konversation
JP	Japan	Rest of Asia Pacific
JE	Jersey	Other
JO	Jordan	Rest of Middle East
KZ	Kazakhstan	Other
KE	Kenya	Rest of Africa
KI	Kiribati	Other
XK	Kosovo	Other
KW	Kuwait	Rest of Middle East
KG	Kyrgyzstan	Other
LA	Lao PDR	Rest of Asia Pacific
LV	Latvia	Rest of Central & Eastern Europe
LB	Lebanon	Rest of Middle East
LS	Lesotho	Rest of Africa
LR	Liberia	Rest of Africa
LY	Libya	Rest of Africa
LI	Liechtenstein	Other
LT	Lithuania	Rest of Central & Eastern Europe
LU	Luxembourg	Other
MO	Macao	Other

Zweistelliger ISO-Ländercode	Ländername	WhatsApp Region für die Abrechnung der Konversation
MK	Macedonia	Rest of Central & Eastern Europe
MG	Madagascar	Rest of Africa
MW	Malawi	Rest of Africa
MY	Malaysia	Malaysia
MV	Maldives	Other
ML	Mali	Rest of Africa
MT	Malta	Other
MH	Marshall Islands	Other
MQ	Martinique	Other
MR	Mauritania	Rest of Africa
MU	Mauritius	Other
YT	Mayotte	Other
MX	Mexico	Mexico
FM	Micronesia	Other
MD	Moldova	Rest of Central & Eastern Europe
MC	Monaco	Other
MN	Mongolia	Rest of Asia Pacific
ME	Montenegro	Other
MS	Montserrat	Other

Zweistelliger ISO-Ländercode	Ländername	WhatsApp Region für die Abrechnung der Konversation
MA	Morocco	Rest of Africa
MZ	Mozambique	Rest of Africa
MM	Myanmar	Other
NA	Namibia	Rest of Africa
NR	Nauru	Other
NP	Nepal	Rest of Asia Pacific
NL	Netherlands	Netherlands
NC	New Caledonia	Other
NZ	New Zealand	Rest of Asia Pacific
NI	Nicaragua	Rest of Latin America
NE	Niger	Rest of Africa
NG	Nigeria	Nigeria
NU	Niue	Other
NF	Norfolk Island	Other
MP	Northern Mariana Islands	Other
NO	Norway	Rest of Western Europe
OM	Oman	Rest of Middle East
PK	Pakistan	Pakistan
PW	Palau	Other
PS	Palestinian Territory	Other

Zweistelliger ISO-Ländercode	Ländername	WhatsApp Region für die Abrechnung der Konversation
PA	Panama	Rest of Latin America
PG	Papua New Guinea	Rest of Asia Pacific
PY	Paraguay	Rest of Latin America
PE	Peru	Peru
PH	Philippines	Rest of Asia Pacific
PN	Pitcairn	Other
PL	Poland	Rest of Central & Eastern Europe
PT	Portugal	Rest of Western Europe
PR	Puerto Rico	Rest of Latin America
QA	Qatar	Rest of Middle East
CG	Republic of Congo	Other
RE	Reunion	Other
RO	Romania	Rest of Central & Eastern Europe
RU	Russian Federation	Russia
RW	Rwanda	Rest of Africa
SH	Saint Helena	Other
KN	Saint Kitts and Nevis	Other
LC	Saint Lucia	Other
PM	Saint Pierre and Miquelon	Other

Zweistelliger ISO-Ländercode	Ländername	WhatsApp Region für die Abrechnung der Konversation
VC	Saint Vincent and Grenadines	Other
BL	Saint-Barthelemy	Other
MF	Saint-Martin	Other
WS	Samoa	Other
SM	San Marino	Other
ST	Sao Tome and Principe	Other
SA	Saudi Arabia	Saudi Arabia
SN	Senegal	Rest of Africa
RS	Serbia	Rest of Central & Eastern Europe
SC	Seychelles	Other
SL	Sierra Leone	Rest of Africa
SG	Singapore	Rest of Asia Pacific
SX	Sint Maarten	Other
SK	Slovakia	Rest of Central & Eastern Europe
SI	Slovenia	Rest of Central & Eastern Europe
SB	Solomon Islands	Other
SO	Somalia	Rest of Africa
ZA	South Africa	South Africa

Zweistelliger ISO-Ländercode	Ländername	WhatsApp Region für die Abrechnung der Konversation
GS	South Georgia and the South Sandwich Islands	Other
KR	South Korea	Other
SS	South Sudan	Rest of Africa
ES	Spain	Spain
LK	Sri Lanka	Rest of Asia Pacific
SR	Suriname	Other
SJ	Svalbard and Jan Mayen Islands	Other
SE	Sweden	Rest of Western Europe
CH	Switzerland	Rest of Western Europe
TW	Taiwan	Rest of Asia Pacific
TJ	Tajikistan	Rest of Asia Pacific
TZ	Tanzania	Rest of Africa
TH	Thailand	Rest of Asia Pacific
TL	Timor-Leste	Other
TG	Togo	Rest of Africa
TK	Tokelau	Other
TO	Tonga	Other
TT	Trinidad and Tobago	Other
TA	Tristan da Cunha	Other

Zweistelliger ISO-Ländercode	Ländername	WhatsApp Region für die Abrechnung der Konversation
TN	Tunisia	Rest of Africa
TR	Turkey	Turkey
TM	Turkmenistan	Rest of Asia Pacific
TC	Turks and Caicos Islands	Other
TV	Tuvalu	Other
UG	Uganda	Rest of Africa
UA	Ukraine	Rest of Central & Eastern Europe
AE	United Arab Emirates	United Arab Emirates
GB	United Kingdom	United Kingdom
US	United States	North America
UY	Uruguay	Rest of Latin America
UM	US Minor Outlying Islands	Other
UZ	Uzbekistan	Rest of Asia Pacific
VU	Vanuatu	Other
VA	Vatican City State	Other
VE	Venezuela	Rest of Latin America
VN	Vietnam	Rest of Asia Pacific
VI	Virgin Islands	Other
WF	Wallis and Futuna Islands	Other

Zweistelliger ISO-Ländercode	Ländername	WhatsApp Region für die Abrechnung der Konversation
EH	Western Sahara	Other
YE	Yemen	Rest of Middle East
ZM	Zambia	Rest of Africa
ZW	Zimbabwe	Other

Überwachung von Social Messaging für AWS Endbenutzer

Die Überwachung ist ein wichtiger Bestandteil der Aufrechterhaltung der Zuverlässigkeit, Verfügbarkeit und Leistung von AWS End User Messaging Social und Ihren anderen AWS-Lösungen. AWS bietet die folgenden Überwachungstools, um AWS End User Messaging Social zu beobachten, zu melden, wenn etwas nicht stimmt, und gegebenenfalls automatische Maßnahmen zu ergreifen:

- Amazon CloudWatch überwacht Ihre AWS Ressourcen und die Anwendungen, auf denen Sie laufen, AWS in Echtzeit. Sie können Kennzahlen erfassen und verfolgen, benutzerdefinierte Dashboards erstellen und Alarme festlegen, die Sie benachrichtigen oder Maßnahmen ergreifen, wenn eine bestimmte Metrik einen von Ihnen festgelegten Schwellenwert erreicht. Sie können beispielsweise die CPU-Auslastung oder andere Kennzahlen Ihrer EC2 Amazon-Instances CloudWatch verfolgen und bei Bedarf automatisch neue Instances starten. Weitere Informationen finden Sie im CloudWatch Amazon-Benutzerhandbuch.
- Mit Amazon CloudWatch Logs können Sie Ihre Protokolldateien von EC2 Amazon-Instances und anderen Quellen überwachen CloudTrail, speichern und darauf zugreifen. CloudWatch Logs kann Informationen in den Protokolldateien überwachen und Sie benachrichtigen, wenn bestimmte Schwellenwerte erreicht werden. Sie können Ihre Protokolldaten auch in einem sehr robusten Speicher archivieren. Weitere Informationen finden Sie im Amazon CloudWatch Logs-Benutzerhandbuch.
- AWS CloudTrailerfasst API-Aufrufe und zugehörige Ereignisse, die von oder im Namen Ihres AWS Kontos getätigt wurden, und übermittelt die Protokolldateien an einen von Ihnen angegebenen Amazon S3 S3-Bucket. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Aufrufe erfolgten. Weitere Informationen finden Sie im AWS CloudTrail -Benutzerhandbuch.

Überwachung von Social Messaging für AWS Endbenutzer mit Amazon CloudWatch

Sie können die Nutzung CloudWatch von AWS End User Messaging Social überwachen. Dabei werden Rohdaten gesammelt und zu lesbaren Messwerten verarbeitet, die nahezu in Echtzeit verfügbar sind. Diese Statistiken werden 15 Monate gespeichert, damit Sie auf Verlaufsinformationen zugreifen können und einen besseren Überblick darüber erhalten, wie Ihre Webanwendung oder der Service ausgeführt werden. Sie können auch Alarme einrichten, die auf bestimmte Grenzwerte

achten und Benachrichtigungen senden oder Aktivitäten auslösen, wenn diese Grenzwerte erreicht werden. Weitere Informationen finden Sie im CloudWatch Amazon-Benutzerhandbuch.

Bei AWS End User Messaging Social sollten Sie darauf achten`WhatsAppMessageFeeCount`, ob ein Ausgabenschwellenwert erreicht ist, auch darauf achten `WhatsAppConversationFeeCount` und einen Alarm auslösen.

> **Note**
>
> Bevor Sie die CloudWatch Metriken verwenden können, müssen Sie eine Service-Link-Rolle erstellen.

In den folgenden Tabellen sind die Metriken und Dimensionen aufgeführt, die AWS End User Messaging Social in den `AWS/SocialMessaging` Namespace exportiert.

Metrik	Einheit	Beschreibung
WhatsAppConversationFeeCount	Anzahl	Die Anzahl der WhatsApp Gesprächsgebühren
WhatsAppMessageFeeCount	Anzahl	Die Anzahl der WhatsApp Nachrichtengebühren
MetaTemplateMessageFeeCount	Anzahl	Die Anzahl der Gebühren für Meta-Template-Nachrichten

> **Note**
>
> Die WhatsAppConversationFeeCount Metrik ist ab dem 1. Juli 2025 nicht mehr verfügbar.

Dimension	Beschreibung
MessageFeeType	Gültige Gebührentypen sind Standard
DestinationCountryCode	Der zweibuchstabige ISO-Code für das Land

Dimension	Beschreibung
WhatsAppPhoneNumberArn	Der ARN der Telefonnummer
MetaTemplateMessageFeeType	Gültige Gebührentypen sind regulär, free_customer_service und free_entry_point
MetaTemplateMessageFeeCategory	Gültige Gebührenkategorien sind Service, Marketing, Nützlichkeit, Authentifizierung und Authentication_International
ConversationFeeType	Gültige Gebührenkategorien sind Service, Marketing, Utility, Authentication und authentication_international

> **Note**
>
> Die ConversationFeeType Dimension ist ab dem 1. Juli 2025 nicht mehr verfügbar.

Protokollieren von Social API-Aufrufen für AWS Endbenutzer-Messaging mithilfe von AWS CloudTrail

AWS End User Messaging Social ist in einen Dienst integriert AWS CloudTrail, der eine Aufzeichnung der von einem Benutzer, einer Rolle oder einem ausgeführten Aktionen bereitstellt AWS-Service. CloudTrail erfasst alle API-Aufrufe für AWS End User Messaging Social als Ereignisse. Zu den erfassten Aufrufen gehören Aufrufe von der AWS End User Messaging Social Console und Code-Aufrufe der AWS End User Messaging Social API-Operationen. Anhand der von gesammelten Informationen können Sie die Anfrage CloudTrail, die an AWS End User Messaging Social gestellt wurde, die IP-Adresse, von der aus die Anfrage gestellt wurde, wann sie gestellt wurde, und weitere Details ermitteln.

Jeder Ereignis- oder Protokolleintrag enthält Informationen zu dem Benutzer, der die Anforderung generiert hat. Die Identitätsinformationen unterstützen Sie bei der Ermittlung der folgenden Punkte:

- Ob die Anfrage mit Anmeldeinformationen des Root-Benutzers oder des Benutzers gestellt wurde.
- Die Anforderung wurde im Namen eines IAM-Identity-Center-Benutzers erstellt.

- Gibt an, ob die Anforderung mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen Verbundbenutzer gesendet wurde.
- Ob die Anforderung aus einem anderen AWS-Service gesendet wurde.

CloudTrail ist in Ihrem aktiv AWS-Konto , wenn Sie das Konto erstellen, und Sie haben automatisch Zugriff auf den CloudTrail Eventverlauf. Der CloudTrail Ereignisverlauf bietet eine einsehbare, durchsuchbare, herunterladbare und unveränderliche Aufzeichnung der aufgezeichneten Verwaltungsereignisse der letzten 90 Tage in einem. AWS-Region Weitere Informationen finden Sie im AWS CloudTrail Benutzerhandbuch unter Arbeiten mit dem CloudTrail Ereignisverlauf. Für die Anzeige des Eventverlaufs CloudTrail fallen keine Gebühren an.

Für eine fortlaufende Aufzeichnung der Ereignisse in AWS-Konto den letzten 90 Tagen erstellen Sie einen Trail- oder CloudTrailLake-Event-Datenspeicher.

CloudTrail Pfade

Ein Trail ermöglicht CloudTrail die Übermittlung von Protokolldateien an einen Amazon S3 S3-Bucket. Alle mit dem erstellten Pfade AWS Management Console sind regionsübergreifend. Sie können mithilfe von AWS CLI einen Einzel-Region- oder einen Multi-Region-Trail erstellen. Es wird empfohlen, einen Trail mit mehreren Regionen zu erstellen, da Sie alle Aktivitäten AWS-Regionen in Ihrem Konto erfassen. Wenn Sie einen Einzel-Region-Trail erstellen, können Sie nur die Ereignisse anzeigen, die im AWS-Region des Trails protokolliert wurden. Weitere Informationen zu Trails finden Sie unter Erstellen eines Trails für Ihr AWS-Konto und Erstellen eines Trails für eine Organisation im AWS CloudTrail -Benutzerhandbuch.

Sie können eine Kopie Ihrer laufenden Verwaltungsereignisse kostenlos an Ihren Amazon S3 S3-Bucket senden, CloudTrail indem Sie einen Trail erstellen. Es fallen jedoch Amazon S3 S3-Speichergebühren an. Weitere Informationen zur CloudTrail Preisgestaltung finden Sie unter AWS CloudTrail Preise. Informationen zu Amazon-S3-Preisen finden Sie unter Amazon S3 – Preise.

CloudTrail Datenspeicher für Ereignisse in Lake

CloudTrail Mit Lake können Sie SQL-basierte Abfragen für Ihre Ereignisse ausführen. CloudTrail Lake konvertiert bestehende Ereignisse im zeilenbasierten JSON-Format in das Apache ORC-Format. ORC ist ein spaltenförmiges Speicherformat, das für den schnellen Abruf von Daten optimiert ist. Die Ereignisse werden in Ereignisdatenspeichern zusammengefasst, bei denen es sich um unveränderliche Sammlungen von Ereignissen handelt, die auf Kriterien basieren, die Sie mit Hilfe von erweiterten Ereignisselektoren auswählen. Die Selektoren, die Sie auf einen Ereignisdatenspeicher anwenden, steuern, welche Ereignisse bestehen bleiben und für Sie zur

Abfrage verfügbar sind. Weitere Informationen zu CloudTrail Lake finden Sie unter Arbeiten mit AWS CloudTrail Lake im AWS CloudTrail Benutzerhandbuch.

CloudTrail Für das Speichern und Abfragen von Ereignisdaten in Lake fallen Kosten an. Beim Erstellen eines Ereignisdatenspeichers wählen Sie die Preisoption aus, die für den Ereignisdatenspeicher genutzt werden soll. Die Preisoption bestimmt die Kosten für die Erfassung und Speicherung von Ereignissen sowie die standardmäßige und maximale Aufbewahrungsdauer für den Ereignisdatenspeicher. Weitere Informationen zur CloudTrail Preisgestaltung finden Sie unter AWS CloudTrail Preise.

AWS Nachrichten für Endbenutzer, Ereignisse im Zusammenhang mit sozialen Daten in CloudTrail

Datenereignisse liefern Informationen über die Ressourcenoperationen, die auf oder in einer Ressource ausgeführt werden (z. B. Lesen oder Schreiben in ein Amazon-S3-Objekt). Sie werden auch als Vorgänge auf Datenebene bezeichnet. Datenereignisse sind oft Aktivitäten mit hohem Volume. Protokolliert standardmäßig CloudTrail keine Datenereignisse. Der CloudTrail Ereignisverlauf zeichnet keine Datenereignisse auf.

Für Datenereignisse werden zusätzliche Gebühren fällig. Weitere Informationen zur CloudTrail Preisgestaltung finden Sie unter AWS CloudTrail Preisgestaltung.

Sie können Datenereignisse für die Ressourcentypen AWS End User Messaging Social mithilfe der CloudTrail Konsole oder CloudTrail API-Operationen protokollieren. AWS CLI Weitere Informationen zum Protokollieren von Datenereignissen finden Sie unter Protokollieren von Datenereignissen mit dem AWS Management Console und Protokollieren von Datenereignissen mit dem AWS Command Line Interface im AWS CloudTrail -Benutzerhandbuch.

In der folgenden Tabelle sind die Ressourcentypen für AWS End User Messaging Social aufgeführt, für die Sie Datenereignisse protokollieren können. In der Spalte Datenereignistyp (Konsole) wird der Wert angezeigt, den Sie in der Liste Datenereignistyp auf der CloudTrail Konsole auswählen können. In der Wertspalte resources.type wird der `resources.type` Wert angezeigt, den Sie bei der Konfiguration erweiterter Event-Selektoren mithilfe von oder angeben würden. AWS CLI CloudTrail APIs In der CloudTrail Spalte APIs Protokollierte Daten werden die API-Aufrufe angezeigt, die CloudTrail für den Ressourcentyp protokolliert wurden.

Typ des Datenereignisses (Konsole)	resources.type-Wert	Daten, die APIs protokolliert wurden CloudTrail
ID der Telefonnummer für soziale Nachrichten	`AWS::SocialMessaging::PhoneNumberId`	• DeleteWhatsAppMessageMedia • GetWhatsAppMessageMedia • PostWhatsAppMessageMedia • SendWhatsAppMessage

Sie können erweiterte Event-Selektoren so konfigurieren, dass sie nach den Feldern `eventName`, `readOnly` und `resources.ARN` filtern, sodass nur die Ereignisse protokolliert werden, die für Sie wichtig sind. Weitere Informationen zu diesen Feldern finden Sie unter AdvancedFieldSelector in der API-Referenz zu AWS CloudTrail

AWS Nachrichten für Endbenutzer, Ereignisse zur Verwaltung von sozialen Netzwerken in CloudTrail

Verwaltungsereignisse enthalten Informationen zu Verwaltungsvorgängen, die an Ressourcen in Ihrem ausgeführt werden AWS-Konto. Sie werden auch als Vorgänge auf Steuerebene bezeichnet. CloudTrail Protokolliert standardmäßig Verwaltungsereignisse.

AWS End User Messaging Social protokolliert alle Vorgänge auf der Steuerungsebene von AWS End User Messaging Social als Verwaltungsereignisse. Eine Liste der Vorgänge auf der Steuerungsebene von AWS End User Messaging Social, bei denen sich AWS End User Messaging Social anmeldet CloudTrail, finden Sie in der Referenz zur AWS End User Messaging Social API.

AWS Beispiele für Ereignisse im Bereich End User Messaging Social

Ein Ereignis stellt eine einzelne Anfrage aus einer beliebigen Quelle dar und enthält Informationen über den angeforderten API-Vorgang, Datum und Uhrzeit des Vorgangs, Anforderungsparameter usw. CloudTrail Protokolldateien sind kein geordneter Stack-Trace der öffentlichen API-Aufrufe, sodass Ereignisse nicht in einer bestimmten Reihenfolge angezeigt werden.

Das folgende Beispiel zeigt ein CloudTrail Ereignis, das den Vorgang demonstriert.

```
{
        "eventVersion": "1.09",
        "userIdentity": {
            "type": "AssumedRole",
            "principalId": "GR632462JDSBDSHHGS39:session",
            "arn": "arn:aws:sts::123456789101:assumed-role/Role_name/Session_name",
            "accountId": "123456789101",
            "accessKeyId": "12345678901234567890",
            "sessionContext": {
                "sessionIssuer": {
                    "type": "Role",
                    "principalId": "GR632462JDSBDEXAMPLE",
                    "arn": "arn:aws:sts::123456789101:assumed-role/Role_name/
Session_name",
                    "accountId": "123456789101",
                    "userName": "user"
                },
                "attributes": {
                    "creationDate": "2024-10-03T17:25:08Z",
                    "mfaAuthenticated": "false"
                }
            }
        },
        "eventTime": "2024-10-03T17:25:23Z",
        "eventSource": "social-messaging.amazonaws.com",
        "eventName": "SendWhatsAppMessage",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "1.x.x.x",
        "userAgent": "agent",
        "requestParameters": {
            "originationPhoneNumberId": "phone-number-id-
aa01234567890123456789012345678 9",
            "metaApiVersion": "v20.0",
            "message": "Hi"
        },
        "responseElements": {
            "messageId": "message_id"
        },
        "requestID": "request_id",
        "eventID": "event_id",
        "readOnly": false,
        "resources": [{
            "accountId": "123456789101",
```

```
            "type": "AWS::SocialMessaging::PhoneNumberId",
            "ARN": "arn:aws:social-messaging:us-east-1:123456789101:phone-number-id/
phone-number-id-aa01234567890123456789012345678 9"
        }],
        "eventType": "AwsApiCall",
        "managementEvent": false,
        "recipientAccountId": "123456789101",
        "eventCategory": "Data",
        "tlsDetails": {
            "clientProvidedHostHeader": "social-messaging.us-east-1.amazonaws.com"
        }
    }
```

Informationen zu CloudTrail Datensatzinhalten finden Sie im AWS CloudTrail Benutzerhandbuch unter CloudTrailDatensatzinhalt.

Bewährte Methoden für Social Messaging für AWS Endbenutzer

In diesem Abschnitt werden mehrere bewährte Methoden beschrieben, die Ihnen helfen können, Ihre Kundenbindung zu verbessern und eine Kontosperrung zu vermeiden. Beachten Sie jedoch, dass diesem Abschnitt keine Rechtsberatung darstellt. Wenden Sie sich immer an einen Rechtsanwalt, um juristischen Rat einzuholen.

Die aktuelle Liste der WhatsApp bewährten Methoden finden Sie in der WhatsApp Business Messaging-Richtlinie.

Themen

Up-to-date Unternehmensprofil

Pflegen Sie ein genaues up-to-date WhatsApp Geschäftsprofil, das Kontaktinformationen für den Kundensupport enthält, z. B. eine E-Mail-Adresse, eine Website-Adresse oder eine Telefonnummer. Stellen Sie sicher, dass die bereitgestellten Informationen der Wahrheit entsprechen und nicht falsch darstellen oder sich als ein anderes Unternehmen ausgeben.

Einholen von Berechtigungen

Senden Sie niemals Nachrichten an Empfänger, die nicht ausdrücklich darum gebeten haben, die Arten von Nachrichten zu erhalten, die Sie senden möchten. Behalten Sie die folgenden Opt-in-Informationen bei:

- Der Opt-in-Prozess muss die Person eindeutig darüber informieren, dass sie damit einverstanden ist, Nachrichten oder Anrufe von Ihrem Unternehmen zu erhalten. WhatsApp Sie müssen den Namen Ihres Unternehmens ausdrücklich angeben.

- Sie sind allein dafür verantwortlich, die Methode zur Einholung der Einwilligung festzulegen. Stellen Sie sicher, dass das Opt-In-Verfahren allen geltenden Gesetzen entspricht, die Ihre Kommunikation regeln. Stellen Sie alle erforderlichen Hinweise bereit und holen Sie alle erforderlichen Genehmigungen gemäß den geltenden Gesetzen ein.

Weitere Informationen zu den WhatsApp Opt-in-Anforderungen finden Sie unter Opt-In einholen für WhatsApp

Wenn sich Empfänger über ein Online-Formular für den Empfang Ihrer Nachrichten anmelden können, verhindern Sie, dass automatisierte Skripte Personen ohne deren Wissen abonnieren. Beschränken Sie außerdem, wie oft ein Benutzer in einer einzigen Sitzung eine Telefonnummer angeben kann.

Respektieren Sie alle Anfragen einer Person, unabhängig davon, ob diese Person aktiviert oder deaktiviert WhatsApp ist, die Kommunikation zu blockieren, zu beenden oder anderweitig abzulehnen, einschließlich der Entfernung dieser Person aus Ihrer Kontaktliste.

Führen Sie Unterlagen mit Datum, Uhrzeit und Quelle der einzelnen Opt-in-Anfragen und Bestätigungen. Dies kann Ihnen auch dabei helfen, routinemäßige Audits Ihrer Kundenliste durchzuführen.

Unzulässiger Nachrichteninhalt

Important

Arbeiten mit Meta/ WhatsApp

- Ihre Nutzung der WhatsApp Business Solution unterliegt den Bedingungen der Nutzungsbedingungen für Unternehmen, den Nutzungsbedingungen für WhatsApp Business Solution, der WhatsApp Business Messaging-Richtlinie, den WhatsApp Messaging-Richtlinien und allen anderen Bestimmungen, Richtlinien oder Richtlinien, die durch Bezugnahme darin enthalten sind (die jeweils von Zeit zu Zeit aktualisiert werden können). WhatsApp
- Meta oder WhatsApp kann Ihnen jederzeit die Nutzung der WhatsApp Business Solution verbieten.

- Im Zusammenhang mit Ihrer Nutzung der WhatsApp Business Solution werden Sie keine Inhalte, Informationen oder Daten einreichen, die gemäß den geltenden Gesetzen oder Vorschriften Schutzmaßnahmen oder Vertriebsbeschränkungen unterliegen.

Wenn Sie gegen die WhatsApp Richtlinie verstoßen, kann Ihr Konto für einen bestimmten Zeitraum vom Senden von Nachrichten blockiert werden, bis Sie Widerspruch einlegen, oder es kann dauerhaft gesperrt werden. Meta informiert dich per E-Mail und an den WhatsApp Business Manager, falls eines deiner Konten oder Vermögenswerte gegen die Richtlinie verstoßen hat. Alle Einsprüche müssen bei Meta eingelegt werden. Informationen zum Anzeigen eines Verstoßes gegen die Richtlinie oder zum Einlegen eines Rechtsbehelfs bei Meta finden Sie unter Informationen zu Richtlinienverstößen für Ihr WhatsApp Unternehmenskonto anzeigen im Meta Business Help Center. Die aktuelle Liste der verbotenen Nachrichteninhalte finden Sie in der WhatsApp Business Messaging-Richtlinie.

Im Folgenden sind die Kategorien verbotener Inhalte für alle Nachrichtentypen weltweit aufgeführt. Wenn du eine Nachricht mit sendest WhatsApp, befolge diese Richtlinien:

Kategorie	Beispiele
Glücksspiel	• Casinos • Gewinnspiele • Apps/Websites
Finanzdienstleistungen mit hoher Risikostufe	• Zahltagdarlehen • Kurzfristige Zinsdarlehen • Autodarlehen • Hypothekendarlehen • Studentendarlehen • Inkasso • Aktienwarnungen • Kryptowährung
Schuldenerlass	• Schuldenkonsolidierung • Schuldenabbau

Kategorie	Beispiele
	• Bonitätsverbesserung
Get-rich-quick Schemata	• Work-from-home programme • Risiko-Investitionschancen • Pyramiden- oder mehrstufige Vermarktu ngssysteme
Illegale Substanzen	• Cannabis/CBD
Phishing/Smishing	• Versuche, Benutzer dazu zu bringen, persönliche Informationen oder Website-L ogin-Informationen offenzulegen.
S.H.A.F.T.	• Sex • Hass • Alkohol • Schusswaffen • Tabak/E-Zigaretten
Generierung von Leads durch Dritte	• Unternehmen, die Verbraucherinformationen kaufen, verkaufen oder weitergeben

Prüfung Ihrer Kundenlisten

Wenn Sie wiederkehrende WhatsApp Nachrichten senden, überprüfen Sie Ihre Kundenlisten regelmäßig. Durch die Prüfung Ihrer Kundenlisten können Sie sicherstellen, dass nur Kunden Ihre Nachrichten erhalten, die sie auch erhalten möchten.

Senden Sie bei der Prüfung Ihrer Liste jedem angemeldeten Kunden eine Nachricht, die diesen an sein Abonnement erinnert, begleitet von Anleitungen zum eventuellen Abbestellen der Nachrichten.

Anpassen Ihres Sendens basierend auf der Kundenbeteiligung

Die Prioritäten Ihrer Kunden können sich mit der Zeit ändern. Wenn Kunden Ihre Nachrichten nicht mehr nützlich finden, bestellen sie sie möglicherweise ganz ab oder melden sie sogar

als unerwünscht. Daher ist es wichtig, dass Sie Ihr Sendeverhalten auf der Grundlage der Kundenbeteiligung anpassen.

Für Kunden, die nur selten mit Ihren Nachrichten interagieren, sollten Sie die Häufigkeit Ihrer Nachrichten entsprechend anpassen. Wenn Sie z. B. wöchentliche Nachrichten an interessierte Kunden senden, können Sie für weniger interessierte Kunden einen monatlichen Kurzbericht erstellen.

Entfernen Sie schließlich Kunden, die niemals mit Ihren Nachrichten interagieren, vollständig aus Ihren Kundenlisten. Dieser Schritt wird verhindert, dass die Kunden irgend wann verärgert auf Ihre Nachrichten reagieren. Außerdem sparen Sie dadurch Geld und schützen Ihren guten Ruf als Sender.

Senden zu angemessenen Zeiten

Senden Sie Nachrichten während der normalen Geschäftszeiten am Tag. Wenn Sie Nachrichten zum Abendessen oder mitten in der Nacht senden, besteht eine gute Chance, dass sich Ihre Kunden von Ihren Listen abmelden, um nicht gestört zu werden. Möglicherweise möchten Sie vermeiden, WhatsApp Nachrichten zu senden, wenn Ihre Kunden nicht sofort darauf antworten können.

Sicherheit bei AWS Endbenutzer-Nachrichten in Social

Cloud-Sicherheit AWS hat höchste Priorität. Als AWS Kunde profitieren Sie von Rechenzentren und Netzwerkarchitekturen, die darauf ausgelegt sind, die Anforderungen der sicherheitssensibelsten Unternehmen zu erfüllen.

Sicherheit ist eine gemeinsame AWS Verantwortung von Ihnen und Ihnen. Das Modell der geteilten Verantwortung beschreibt dies als Sicherheit der Cloud selbst und Sicherheit in der Cloud:

- Sicherheit der Cloud — AWS ist verantwortlich für den Schutz der Infrastruktur, auf der AWS Dienste in der ausgeführt AWS Cloud werden. AWS bietet Ihnen auch Dienste, die Sie sicher nutzen können. Externe Prüfer testen und verifizieren regelmäßig die Wirksamkeit unserer Sicherheitsmaßnahmen im Rahmen der AWS . Weitere Informationen zu den Compliance-Programmen, die für AWS End User Messaging Social gelten, finden Sie unter AWS Services im Umfang nach Compliance-Programm AWS .
- Sicherheit in der Cloud — Ihre Verantwortung richtet sich nach dem AWS Dienst, den Sie nutzen. Sie sind auch für andere Faktoren verantwortlich, etwa für die Vertraulichkeit Ihrer Daten, für die Anforderungen Ihres Unternehmens und für die geltenden Gesetze und Vorschriften.

Diese Dokumentation hilft Ihnen zu verstehen, wie Sie das Modell der gemeinsamen Verantwortung bei der Verwendung von AWS End User Messaging Social anwenden können. In den folgenden Themen erfahren Sie, wie Sie AWS End User Messaging Social konfigurieren, um Ihre Sicherheits- und Compliance-Ziele zu erreichen. Sie erfahren auch, wie Sie andere AWS Dienste verwenden können, die Ihnen helfen, Ihre AWS End User Messaging Social-Ressourcen zu überwachen und zu schützen.

Themen

- Verwenden von dienstbezogenen Rollen für AWS End User Messaging Social

Datenschutz in AWS End User Messaging Social

Das AWS Modell der mit gilt für den Datenschutz in AWS End User Messaging Social. Wie in diesem Modell beschrieben, AWS ist verantwortlich für den Schutz der globalen Infrastruktur, auf der alle Systeme laufen AWS Cloud. Sie sind dafür verantwortlich, die Kontrolle über Ihre in dieser Infrastruktur gehosteten Inhalte zu behalten. Sie sind auch für die Sicherheitskonfiguration und die Verwaltungsaufgaben für die von Ihnen verwendeten AWS-Services verantwortlich. Weitere Informationen zum Datenschutz finden Sie unter Häufig gestellte Fragen zum Datenschutz. Informationen zum Datenschutz in Europa finden Sie im Blog-Beitrag AWS -Modell der geteilten Verantwortung und in der DSGVO im AWS -Sicherheitsblog.

Aus Datenschutzgründen empfehlen wir, dass Sie AWS-Konto Anmeldeinformationen schützen und einzelne Benutzer mit AWS IAM Identity Center oder AWS Identity and Access Management (IAM) einrichten. So erhält jeder Benutzer nur die Berechtigungen, die zum Durchführen seiner Aufgaben erforderlich sind. Außerdem empfehlen wir, die Daten mit folgenden Methoden schützen:

- Verwenden Sie für jedes Konto die Multi-Faktor-Authentifizierung (MFA).
- Wird verwendet SSL/TLS , um mit AWS Ressourcen zu kommunizieren. Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Richten Sie die API und die Protokollierung von Benutzeraktivitäten mit ein AWS CloudTrail. Informationen zur Verwendung von CloudTrail Pfaden zur Erfassung von AWS Aktivitäten finden Sie unter Arbeiten mit CloudTrail Pfaden im AWS CloudTrail Benutzerhandbuch.
- Verwenden Sie AWS Verschlüsselungslösungen zusammen mit allen darin enthaltenen Standardsicherheitskontrollen AWS-Services.
- Verwenden Sie erweiterte verwaltete Sicherheitsservices wie Amazon Macie, die dabei helfen, in Amazon S3 gespeicherte persönliche Daten zu erkennen und zu schützen.
- Wenn Sie für den Zugriff AWS über eine Befehlszeilenschnittstelle oder eine API FIPS 140-3-validierte kryptografische Module benötigen, verwenden Sie einen FIPS-Endpunkt. Weitere Informationen über verfügbare FIPS-Endpunkte finden Sie unter Federal Information Processing Standard (FIPS) 140-3.

Wir empfehlen dringend, in Freitextfeldern, z. B. im Feld Name, keine vertraulichen oder sensiblen Informationen wie die E-Mail-Adressen Ihrer Kunden einzugeben. Dies gilt auch, wenn Sie mit AWS End User Messaging Social oder anderen Programmen AWS-Services über die Konsole,

API oder arbeiten. AWS CLI AWS SDKs Alle Daten, die Sie in Tags oder Freitextfelder eingeben, die für Namen verwendet werden, können für Abrechnungs- oder Diagnoseprotokolle verwendet werden. Wenn Sie eine URL für einen externen Server bereitstellen, empfehlen wir dringend, keine Anmeldeinformationen zur Validierung Ihrer Anforderung an den betreffenden Server in die URL einzuschließen.

> **Important**
>
> WhatsApp verwendet das Signal-Protokoll für sichere Kommunikation. Da es sich bei AWS End User Messaging Social jedoch um einen Drittanbieter handelt, werden diese Nachrichten WhatsApp nicht als end-to-end verschlüsselt betrachtet. Weitere Informationen zum WhatsApp Datenschutz finden Sie im Whitepaper Datenschutz, Sicherheit und WhatsApp Verschlüsselung im Überblick.

Datenverschlüsselung

AWS Endbenutzer-Nachrichten Soziale Daten werden bei der Übertragung und bei der Speicherung innerhalb der AWS Grenzen verschlüsselt. Wenn Sie Daten an AWS End User Messaging Social senden, werden die Daten beim Empfang verschlüsselt und gespeichert. Wenn Sie Daten von AWS End User Messaging Social abrufen, werden die Daten mithilfe aktueller Sicherheitsprotokolle an Sie übertragen.

Verschlüsselung im Ruhezustand

AWS End User Messaging Social verschlüsselt alle Daten, die es für Sie innerhalb der AWS Grenzen speichert. Dazu gehören Konfigurationsdaten, Registrierungsdaten und alle Daten, die Sie zu AWS End User Messaging Social hinzufügen. Um Ihre Daten zu verschlüsseln, verwendet AWS End User Messaging Social interne AWS Key Management Service (AWS KMS) Schlüssel, die der Dienst besitzt und in Ihrem Namen verwaltet. Informationen zu AWS KMS finden Sie im AWS Key Management Service -Developer-Handbuch.

Verschlüsselung während der Übertragung

AWS End User Messaging Social verwendet HTTPS und Transport Layer Security (TLS) 1.2, um mit Ihren Kunden, Anwendungen und Meta zu kommunizieren. Um mit anderen AWS Diensten zu kommunizieren, verwendet AWS End User Messaging Social HTTPS und TLS 1.2. Wenn Sie Ressourcen für AWS End User Messaging Social mithilfe der Konsole, eines AWS SDK oder des

erstellen und verwalten, ist die AWS Command Line Interface gesamte Kommunikation außerdem mit HTTPS und TLS 1.2 gesichert.

Schlüsselverwaltung

Um Ihre Daten zu verschlüsseln, verwendet AWS End User Messaging Social interne AWS KMS Schlüssel, die dem Dienst gehören und in Ihrem Namen verwaltet werden. Diese Schlüssel werden regelmäßig rotiert. Sie können Ihre eigenen AWS KMS oder andere Schlüssel nicht bereitstellen und verwenden, um Daten zu verschlüsseln, die Sie in AWS End User Messaging Social speichern.

Datenschutz für den Datenverkehr zwischen Netzwerken

Datenschutz im Netzwerkverkehr bezieht sich auf die Sicherung von Verbindungen und Datenverkehr zwischen AWS End User Messaging Social und Ihren lokalen Clients und Anwendungen sowie zwischen AWS End User Messaging Social und anderen AWS Ressourcen in demselben Netzwerk. AWS-Region Die folgenden Funktionen und Verfahren können Ihnen dabei helfen, den Datenschutz im Netzwerkverkehr für AWS End User Messaging Social zu schützen.

Datenverkehr zwischen AWS End User Messaging Social und lokalen Clients und Anwendungen

Um eine private Verbindung zwischen AWS End User Messaging Social und Clients und Anwendungen in Ihrem lokalen Netzwerk herzustellen, können Sie verwenden. AWS Direct Connect Auf diese Weise können Sie Ihr Netzwerk mit einem AWS Direct Connect -Standort verbinden, indem Sie ein Standard-Glasfaser-Ethernet-Kabel verwenden. Ein Ende des Kabels ist mit Ihrem Router verbunden. Das andere Ende ist mit einem AWS Direct Connect Router verbunden. Weitere Informationen finden Sie unter Was ist AWS Direct Connect? im AWS Direct Connect - Benutzerhandbuch.

Um den Zugriff auf AWS End User Messaging Social über veröffentlichte Websites zu sichern APIs, empfehlen wir Ihnen, die Anforderungen von AWS End User Messaging Social für API-Aufrufe einzuhalten. AWS Für End User Messaging Social müssen Clients Transport Layer Security (TLS) 1.2 oder höher verwenden. Clients müssen außerdem Cipher Suites mit PFS (Perfect Forward Secrecy) wie DHE (Ephemeral Diffie-Hellman) oder ECDHE (Elliptic Curve Ephemeral Diffie-Hellman) unterstützen. Die meisten modernen Systeme wie Java 7 und höher unterstützen diese Modi.

Darüber hinaus müssen Anfragen mit einer Zugriffsschlüssel-ID und einem geheimen Zugriffsschlüssel signiert werden, der einem AWS Identity and Access Management (IAM-) Prinzipal

für Ihr AWS Konto zugeordnet ist. Alternativ können Sie mit AWS Security Token Service (AWS STS) temporäre Sicherheitsanmeldeinformationen erstellen, um die Anforderungen zu signieren.

Identitäts- und Zugriffsmanagement für AWS End User Messaging Social

AWS Identity and Access Management (IAM) hilft einem Administrator AWS-Service , den Zugriff auf Ressourcen sicher zu AWS kontrollieren. IAM-Administratoren kontrollieren, wer authentifiziert (angemeldet) und autorisiert werden kann (über Berechtigungen verfügt), um die Social Media Ressourcen von AWS End User Messaging zu nutzen. IAM ist ein Programm AWS-Service , das Sie ohne zusätzliche Kosten nutzen können.

Themen

Zielgruppe

Die Art und Weise, wie Sie AWS Identity and Access Management (IAM) verwenden, hängt von der Arbeit ab, die Sie in AWS End User Messaging Social ausführen.

Dienstbenutzer — Wenn Sie den AWS End User Messaging Social-Dienst für Ihre Arbeit verwenden, stellt Ihnen Ihr Administrator die erforderlichen Anmeldeinformationen und Berechtigungen zur Verfügung. Wenn Sie für Ihre Arbeit mehr Funktionen von AWS End User Messaging Social verwenden, benötigen Sie möglicherweise zusätzliche Berechtigungen. Wenn Sie die Funktionsweise der Zugriffskontrolle nachvollziehen, wissen Sie bereits, welche Berechtigungen Sie von Ihrem Administrator anfordern müssen. Wenn Sie auf eine Funktion in AWS End User Messaging Social nicht zugreifen können, finden Sie weitere Informationen unterProblembehebung bei AWS Endbenutzernachrichten Soziale Identität und Zugriff.

Dienstadministrator — Wenn Sie in Ihrem Unternehmen für die Ressourcen von AWS End User Messaging Social verantwortlich sind, haben Sie wahrscheinlich vollen Zugriff auf AWS End User Messaging Social. Es ist Ihre Aufgabe, zu bestimmen, auf welche Funktionen und Ressourcen von AWS End User Messaging Social Ihre Servicebenutzer zugreifen sollen. Anschließend müssen Sie Anforderungen an Ihren IAM-Administrator senden, um die Berechtigungen der Servicebenutzer zu ändern. Lesen Sie die Informationen auf dieser Seite, um die Grundkonzepte von IAM nachzuvollziehen. Weitere Informationen darüber, wie Ihr Unternehmen IAM mit AWS End User Messaging Social verwenden kann, finden Sie unterSo funktioniert AWS End User Messaging Social mit IAM.

IAM-Administrator — Wenn Sie ein IAM-Administrator sind, möchten Sie vielleicht mehr darüber erfahren, wie Sie Richtlinien schreiben können, um den Zugriff auf AWS End User Messaging Social zu verwalten. Beispiele für identitätsbasierte Richtlinien von AWS End User Messaging Social, die Sie in IAM verwenden können, finden Sie unter. Beispiele für identitätsbasierte Richtlinien für AWS End User Messaging Social

Authentifizierung mit Identitäten

Authentifizierung ist die Art und Weise, wie Sie sich AWS mit Ihren Identitätsdaten anmelden. Sie müssen als IAM-Benutzer authentifiziert (angemeldet AWS) sein oder eine IAM-Rolle annehmen. Root-Benutzer des AWS-Kontos

Sie können sich AWS als föderierte Identität anmelden, indem Sie Anmeldeinformationen verwenden, die über eine Identitätsquelle bereitgestellt wurden. AWS IAM Identity Center (IAM Identity Center) -Benutzer, die Single Sign-On-Authentifizierung Ihres Unternehmens und Ihre Google- oder Facebook-Anmeldeinformationen sind Beispiele für föderierte Identitäten. Wenn Sie sich als Verbundidentität anmelden, hat der Administrator vorher mithilfe von IAM-Rollen einen Identitätsverbund eingerichtet. Wenn Sie über den Verbund darauf zugreifen AWS , übernehmen Sie indirekt eine Rolle.

Je nachdem, welcher Benutzertyp Sie sind, können Sie sich beim AWS Management Console oder beim AWS Zugangsportal anmelden. Weitere Informationen zur Anmeldung finden Sie AWS unter So melden Sie sich bei Ihrem an AWS-Konto im AWS-Anmeldung Benutzerhandbuch.

Wenn Sie AWS programmgesteuert zugreifen, AWS stellt es ein Software Development Kit (SDK) und eine Befehlszeilenschnittstelle (CLI) bereit, um Ihre Anfragen mithilfe Ihrer Anmeldeinformationen kryptografisch zu signieren. Wenn Sie keine AWS Tools verwenden, müssen Sie Anfragen selbst signieren. Weitere Informationen zur Verwendung der empfohlenen Methode für die Selbstsignierung

von Anforderungen finden Sie unter AWS Signature Version 4 für API-Anforderungen im IAM-Benutzerhandbuch.

Unabhängig von der verwendeten Authentifizierungsmethode müssen Sie möglicherweise zusätzliche Sicherheitsinformationen bereitstellen. AWS Empfiehlt beispielsweise, die Multi-Faktor-Authentifizierung (MFA) zu verwenden, um die Sicherheit Ihres Kontos zu erhöhen. Weitere Informationen finden Sie unter Multi-Faktor-Authentifizierung im AWS IAM Identity Center - Benutzerhandbuch und AWS Multi-Faktor-Authentifizierung (MFA) in IAM im IAM-Benutzerhandbuch.

AWS-Konto Root-Benutzer

Wenn Sie einen erstellen AWS-Konto, beginnen Sie mit einer Anmeldeidentität, die vollständigen Zugriff auf alle AWS-Services Ressourcen im Konto hat. Diese Identität wird als AWS-Konto Root-Benutzer bezeichnet. Sie können darauf zugreifen, indem Sie sich mit der E-Mail-Adresse und dem Passwort anmelden, mit denen Sie das Konto erstellt haben. Wir raten ausdrücklich davon ab, den Root-Benutzer für Alltagsaufgaben zu verwenden. Schützen Sie Ihre Root-Benutzer-Anmeldeinformationen. Verwenden Sie diese nur, um die Aufgaben auszuführen, die nur der Root-Benutzer ausführen kann. Eine vollständige Liste der Aufgaben, für die Sie sich als Root-Benutzer anmelden müssen, finden Sie unter Aufgaben, die Root-Benutzer-Anmeldeinformationen erfordern im IAM-Benutzerhandbuch.

Verbundidentität

Als bewährte Methode sollten menschliche Benutzer, einschließlich Benutzer, die Administratorzugriff benötigen, für den Zugriff AWS-Services mithilfe temporärer Anmeldeinformationen den Verbund mit einem Identitätsanbieter verwenden.

Eine föderierte Identität ist ein Benutzer aus Ihrem Unternehmensbenutzerverzeichnis, einem Web-Identitätsanbieter AWS Directory Service, dem Identity Center-Verzeichnis oder einem beliebigen Benutzer, der mithilfe AWS-Services von Anmeldeinformationen zugreift, die über eine Identitätsquelle bereitgestellt wurden. Wenn föderierte Identitäten darauf zugreifen AWS-Konten, übernehmen sie Rollen, und die Rollen stellen temporäre Anmeldeinformationen bereit.

Für die zentrale Zugriffsverwaltung empfehlen wir Ihnen, AWS IAM Identity Center zu verwenden. Sie können Benutzer und Gruppen in IAM Identity Center erstellen, oder Sie können eine Verbindung zu einer Gruppe von Benutzern und Gruppen in Ihrer eigenen Identitätsquelle herstellen und diese synchronisieren, um sie in all Ihren AWS-Konten Anwendungen zu verwenden. Informationen zu IAM Identity Center finden Sie unter Was ist IAM Identity Center? im AWS IAM Identity Center - Benutzerhandbuch.

IAM-Benutzer und -Gruppen

Ein IAM-Benutzer ist eine Identität innerhalb Ihres Unternehmens AWS-Konto , die über spezifische Berechtigungen für eine einzelne Person oder Anwendung verfügt. Wenn möglich, empfehlen wir, temporäre Anmeldeinformationen zu verwenden, anstatt IAM-Benutzer zu erstellen, die langfristige Anmeldeinformationen wie Passwörter und Zugriffsschlüssel haben. Bei speziellen Anwendungsfällen, die langfristige Anmeldeinformationen mit IAM-Benutzern erfordern, empfehlen wir jedoch, die Zugriffsschlüssel zu rotieren. Weitere Informationen finden Sie unter Regelmäßiges Rotieren von Zugriffsschlüsseln für Anwendungsfälle, die langfristige Anmeldeinformationen erfordern im IAM-Benutzerhandbuch.

Eine IAM-Gruppe ist eine Identität, die eine Sammlung von IAM-Benutzern angibt. Sie können sich nicht als Gruppe anmelden. Mithilfe von Gruppen können Sie Berechtigungen für mehrere Benutzer gleichzeitig angeben. Gruppen vereinfachen die Verwaltung von Berechtigungen, wenn es zahlreiche Benutzer gibt. Sie könnten beispielsweise eine Gruppe benennen IAMAdminsund dieser Gruppe Berechtigungen zur Verwaltung von IAM-Ressourcen erteilen.

Benutzer unterscheiden sich von Rollen. Ein Benutzer ist einer einzigen Person oder Anwendung eindeutig zugeordnet. Eine Rolle kann von allen Personen angenommen werden, die sie benötigen. Benutzer besitzen dauerhafte Anmeldeinformationen. Rollen stellen temporäre Anmeldeinformationen bereit. Weitere Informationen finden Sie unter Anwendungsfälle für IAM-Benutzer im IAM-Benutzerhandbuch.

IAM-Rollen

Eine IAM-Rolle ist eine Identität innerhalb von Ihnen AWS-Konto , die über bestimmte Berechtigungen verfügt. Sie ist einem IAM-Benutzer vergleichbar, jedoch nicht mit einer bestimmten Person verknüpft. Um vorübergehend eine IAM-Rolle in der zu übernehmen AWS Management Console, können Sie von einer Benutzer- zu einer IAM-Rolle (Konsole) wechseln. Sie können eine Rolle übernehmen, indem Sie eine AWS CLI oder AWS API-Operation aufrufen oder eine benutzerdefinierte URL verwenden. Weitere Informationen zu Methoden für die Verwendung von Rollen finden Sie unter Methoden für die Übernahme einer Rolle im IAM-Benutzerhandbuch.

IAM-Rollen mit temporären Anmeldeinformationen sind in folgenden Situationen hilfreich:

- Verbundbenutzerzugriff – Um einer Verbundidentität Berechtigungen zuzuweisen, erstellen Sie eine Rolle und definieren Berechtigungen für die Rolle. Wird eine Verbundidentität authentifiziert, so wird die Identität der Rolle zugeordnet und erhält die von der Rolle definierten Berechtigungen. Informationen zu Rollen für den Verbund finden Sie unter Erstellen von Rollen für externe

Identitätsanbieter (Verbund) im IAM-Benutzerhandbuch. Wenn Sie IAM Identity Center verwenden, konfigurieren Sie einen Berechtigungssatz. Wenn Sie steuern möchten, worauf Ihre Identitäten nach der Authentifizierung zugreifen können, korreliert IAM Identity Center den Berechtigungssatz mit einer Rolle in IAM. Informationen zu Berechtigungssätzen finden Sie unter Berechtigungssätze im AWS IAM Identity Center -Benutzerhandbuch.

- Temporäre IAM-Benutzerberechtigungen – Ein IAM-Benutzer oder eine -Rolle kann eine IAM-Rolle übernehmen, um vorübergehend andere Berechtigungen für eine bestimmte Aufgabe zu erhalten.
- Kontoübergreifender Zugriff – Sie können eine IAM-Rolle verwenden, um einem vertrauenswürdigen Prinzipal in einem anderen Konto den Zugriff auf Ressourcen in Ihrem Konto zu ermöglichen. Rollen stellen die primäre Möglichkeit dar, um kontoübergreifendem Zugriff zu gewähren. Bei einigen können Sie AWS-Services jedoch eine Richtlinie direkt an eine Ressource anhängen (anstatt eine Rolle als Proxy zu verwenden). Informationen zu den Unterschieden zwischen Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie unter Kontoübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch.
- Serviceübergreifender Zugriff — Einige AWS-Services verwenden Funktionen in anderen AWS-Services. Wenn Sie beispielsweise in einem Service einen Anruf tätigen, ist es üblich, dass dieser Service Anwendungen in Amazon ausführt EC2 oder Objekte in Amazon S3 speichert. Ein Dienst kann dies mit den Berechtigungen des aufrufenden Prinzipals mit einer Servicerolle oder mit einer serviceverknüpften Rolle tun.
  - Forward Access Sessions (FAS) — Wenn Sie einen IAM-Benutzer oder eine IAM-Rolle verwenden, um Aktionen auszuführen AWS, gelten Sie als Principal. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service initiieren. FAS verwendet die Berechtigungen des Prinzipals, der einen aufruft AWS-Service, in Kombination mit der Anfrage, Anfragen an AWS-Service nachgelagerte Dienste zu stellen. FAS-Anfragen werden nur gestellt, wenn ein Dienst eine Anfrage erhält, für deren Abschluss Interaktionen mit anderen AWS-Services oder Ressourcen erforderlich sind. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen. Einzelheiten zu den Richtlinien für FAS-Anfragen finden Sie unter Zugriffssitzungen weiterleiten.
  - Servicerolle – Eine Servicerolle ist eine IAM-Rolle, die ein Service übernimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM-Administrator kann eine Servicerolle innerhalb von IAM erstellen, ändern und löschen. Weitere Informationen finden Sie unter Erstellen einer Rolle zum Delegieren von Berechtigungen an einen AWS-Service im IAM-Benutzerhandbuch.
  - Dienstbezogene Rolle — Eine dienstbezogene Rolle ist eine Art von Servicerolle, die mit einer verknüpft ist. AWS-Service Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Servicebezogene Rollen erscheinen in Ihrem Dienst AWS-Konto und

gehören dem Dienst. Ein IAM-Administrator kann die Berechtigungen für Service-verknüpfte Rollen anzeigen, aber nicht bearbeiten.

- Auf Amazon ausgeführte Anwendungen EC2 — Sie können eine IAM-Rolle verwenden, um temporäre Anmeldeinformationen für Anwendungen zu verwalten, die auf einer EC2 Instance ausgeführt werden und AWS API-Anfragen stellen AWS CLI . Dies ist dem Speichern von Zugriffsschlüsseln innerhalb der EC2 Instance vorzuziehen. Um einer EC2 Instanz eine AWS Rolle zuzuweisen und sie allen ihren Anwendungen zur Verfügung zu stellen, erstellen Sie ein Instanzprofil, das an die Instanz angehängt ist. Ein Instanzprofil enthält die Rolle und ermöglicht Programmen, die auf der EC2 Instanz ausgeführt werden, temporäre Anmeldeinformationen abzurufen. Weitere Informationen finden Sie im IAM-Benutzerhandbuch unter Verwenden einer IAM-Rolle, um Berechtigungen für Anwendungen zu gewähren, die auf EC2 Amazon-Instances ausgeführt werden.

Verwalten des Zugriffs mit Richtlinien

Sie kontrollieren den Zugriff, AWS indem Sie Richtlinien erstellen und diese an AWS Identitäten oder Ressourcen anhängen. Eine Richtlinie ist ein Objekt, AWS das, wenn es einer Identität oder Ressource zugeordnet ist, deren Berechtigungen definiert. AWS wertet diese Richtlinien aus, wenn ein Prinzipal (Benutzer, Root-Benutzer oder Rollensitzung) eine Anfrage stellt. Die Berechtigungen in den Richtlinien legen fest, ob eine Anforderung zugelassen oder abgelehnt wird. Die meisten Richtlinien werden AWS als JSON-Dokumente gespeichert. Weitere Informationen zu Struktur und Inhalten von JSON-Richtliniendokumenten finden Sie unter Übersicht über JSON-Richtlinien im IAM-Benutzerhandbuch.

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer auf was Zugriff hat. Das heißt, welcher Prinzipal Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen kann.

Standardmäßig haben Benutzer, Gruppen und Rollen keine Berechtigungen. Ein IAM-Administrator muss IAM-Richtlinien erstellen, die Benutzern die Berechtigung erteilen, Aktionen für die Ressourcen auszuführen, die sie benötigen. Der Administrator kann dann die IAM-Richtlinien zu Rollen hinzufügen, und Benutzer können die Rollen annehmen.

IAM-Richtlinien definieren Berechtigungen für eine Aktion unabhängig von der Methode, die Sie zur Ausführung der Aktion verwenden. Angenommen, es gibt eine Richtlinie, die Berechtigungen für die `iam:GetRole`-Aktion erteilt. Ein Benutzer mit dieser Richtlinie kann Rolleninformationen von der AWS Management Console AWS CLI, der oder der AWS API abrufen.

Identitätsbasierte Richtlinien

Identitätsbasierte Richtlinien sind JSON-Berechtigungsrichtliniendokumente, die Sie einer Identität anfügen können, wie z. B. IAM-Benutzern, -Benutzergruppen oder -Rollen. Diese Richtlinien steuern, welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen identitätsbasierter Richtlinien finden Sie unter Definieren benutzerdefinierter IAM-Berechtigungen mit vom Kunden verwalteten Richtlinien im IAM-Benutzerhandbuch.

Identitätsbasierte Richtlinien können weiter als Inline-Richtlinien oder verwaltete Richtlinien kategorisiert werden. Inline-Richtlinien sind direkt in einen einzelnen Benutzer, eine einzelne Gruppe oder eine einzelne Rolle eingebettet. Verwaltete Richtlinien sind eigenständige Richtlinien, die Sie mehreren Benutzern, Gruppen und Rollen in Ihrem System zuordnen können AWS-Konto. Zu den verwalteten Richtlinien gehören AWS verwaltete Richtlinien und vom Kunden verwaltete Richtlinien. Informationen dazu, wie Sie zwischen einer verwalteten Richtlinie und einer Inline-Richtlinie wählen, finden Sie unter Auswählen zwischen verwalteten und eingebundenen Richtlinien im IAM-Benutzerhandbuch.

Ressourcenbasierte Richtlinien

Ressourcenbasierte Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anfügen. Beispiele für ressourcenbasierte Richtlinien sind IAM-Rollen-Vertrauensrichtlinien und Amazon-S3-Bucket-Richtlinien. In Services, die ressourcenbasierte Richtlinien unterstützen, können Service-Administratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource zu steuern. Für die Ressource, an welche die Richtlinie angehängt ist, legt die Richtlinie fest, welche Aktionen ein bestimmter Prinzipal unter welchen Bedingungen für diese Ressource ausführen kann. Sie müssen in einer ressourcenbasierten Richtlinie einen Prinzipal angeben. Zu den Prinzipalen können Konten, Benutzer, Rollen, Verbundbenutzer oder gehören. AWS-Services

Ressourcenbasierte Richtlinien sind Richtlinien innerhalb dieses Diensts. Sie können AWS verwaltete Richtlinien von IAM nicht in einer ressourcenbasierten Richtlinie verwenden.

Zugriffskontrolllisten () ACLs

Zugriffskontrolllisten (ACLs) steuern, welche Principals (Kontomitglieder, Benutzer oder Rollen) über Zugriffsberechtigungen für eine Ressource verfügen. ACLs ähneln ressourcenbasierten Richtlinien, verwenden jedoch nicht das JSON-Richtliniendokumentformat.

Amazon S3 und Amazon VPC sind Beispiele für Dienste, die Unterstützung ACLs bieten. AWS WAF Weitere Informationen finden Sie unter Übersicht über ACLs die Zugriffskontrollliste (ACL) im Amazon Simple Storage Service Developer Guide.

Weitere Richtlinientypen

AWS unterstützt zusätzliche, weniger verbreitete Richtlinientypen. Diese Richtlinientypen können die maximalen Berechtigungen festlegen, die Ihnen von den häufiger verwendeten Richtlinientypen erteilt werden können.

- Berechtigungsgrenzen – Eine Berechtigungsgrenze ist ein erweitertes Feature, mit der Sie die maximalen Berechtigungen festlegen können, die eine identitätsbasierte Richtlinie einer IAM-Entität (IAM-Benutzer oder -Rolle) erteilen kann. Sie können eine Berechtigungsgrenze für eine Entität festlegen. Die daraus resultierenden Berechtigungen sind der Schnittpunkt der identitätsbasierten Richtlinien einer Entität und ihrer Berechtigungsgrenzen. Ressourcenbasierte Richtlinien, die den Benutzer oder die Rolle im Feld `Principal` angeben, werden nicht durch Berechtigungsgrenzen eingeschränkt. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen über Berechtigungsgrenzen finden Sie unter Berechtigungsgrenzen für IAM-Entitäten im IAM-Benutzerhandbuch.
- Dienststeuerungsrichtlinien (SCPs) — SCPs sind JSON-Richtlinien, die die maximalen Berechtigungen für eine Organisation oder Organisationseinheit (OU) in festlegen. AWS Organizations AWS Organizations ist ein Dienst zur Gruppierung und zentralen Verwaltung mehrerer Objekte AWS-Konten , die Ihrem Unternehmen gehören. Wenn Sie alle Funktionen in einer Organisation aktivieren, können Sie Richtlinien zur Servicesteuerung (SCPs) auf einige oder alle Ihre Konten anwenden. Das SCP schränkt die Berechtigungen für Entitäten in Mitgliedskonten ein, einschließlich der einzelnen Root-Benutzer des AWS-Kontos Entitäten. Weitere Informationen zu Organizations und SCPs finden Sie unter Richtlinien zur Servicesteuerung im AWS Organizations Benutzerhandbuch.
- Ressourcenkontrollrichtlinien (RCPs) — RCPs sind JSON-Richtlinien, mit denen Sie die maximal verfügbaren Berechtigungen für Ressourcen in Ihren Konten festlegen können, ohne die IAM-Richtlinien aktualisieren zu müssen, die jeder Ressource zugeordnet sind, deren Eigentümer Sie sind. Das RCP schränkt die Berechtigungen für Ressourcen in Mitgliedskonten ein und kann sich auf die effektiven Berechtigungen für Identitäten auswirken, einschließlich der Root-Benutzer des AWS-Kontos, unabhängig davon, ob sie zu Ihrer Organisation gehören. Weitere Informationen zu Organizations RCPs, einschließlich einer Liste AWS-Services dieser Support-Leistungen RCPs, finden Sie unter Resource Control Policies (RCPs) im AWS Organizations Benutzerhandbuch.

- Sitzungsrichtlinien – Sitzungsrichtlinien sind erweiterte Richtlinien, die Sie als Parameter übergeben, wenn Sie eine temporäre Sitzung für eine Rolle oder einen verbundenen Benutzer programmgesteuert erstellen. Die resultierenden Sitzungsberechtigungen sind eine Schnittmenge der auf der Identität des Benutzers oder der Rolle basierenden Richtlinien und der Sitzungsrichtlinien. Berechtigungen können auch aus einer ressourcenbasierten Richtlinie stammen. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen finden Sie unter Sitzungsrichtlinien im IAM-Benutzerhandbuch.

Mehrere Richtlinientypen

Wenn mehrere auf eine Anforderung mehrere Richtlinientypen angewendet werden können, sind die entsprechenden Berechtigungen komplizierter. Informationen darüber, wie AWS bestimmt wird, ob eine Anfrage zulässig ist, wenn mehrere Richtlinientypen betroffen sind, finden Sie im IAM-Benutzerhandbuch unter Bewertungslogik für Richtlinien.

So funktioniert AWS End User Messaging Social mit IAM

Bevor Sie IAM verwenden, um den Zugriff auf AWS End User Messaging Social zu verwalten, sollten Sie sich darüber informieren, welche IAM-Funktionen für die Verwendung mit AWS End User Messaging Social verfügbar sind.

IAM-Funktionen, die Sie mit AWS End User Messaging Social verwenden können

IAM-Feature	AWS Unterstützung für Endbenutzer-Nachrichten in sozialen Netzwerken
Identitätsbasierte Richtlinien	Ja
Ressourcenbasierte Richtlinien	Nein
Richtlinienaktionen	Ja
Richtlinienressourcen	Ja
Bedingungsschlüssel für die Richtlinie	Ja
ACLs	Nein
ABAC (Tags in Richtlinien)	Teilweise

IAM-Feature	AWS Unterstützung für Endbenutzer-Nachrichten in sozialen Netzwerken
Temporäre Anmeldeinformationen	Ja
Prinzipalberechtigungen	Ja
Servicerollen	Ja
Service-verknüpfte Rollen	Ja

Einen allgemeinen Überblick darüber, wie AWS End User Messaging Social und andere AWS Dienste mit den meisten IAM-Funktionen funktionieren, finden Sie im IAM-Benutzerhandbuch unter AWS Dienste, die mit IAM funktionieren.

Identitätsbasierte Richtlinien für End User Messaging Social AWS

Unterstützt Richtlinien auf Identitätsbasis: Ja

Identitätsbasierte Richtlinien sind JSON-Berechtigungsrichtliniendokumente, die Sie einer Identität anfügen können, wie z. B. IAM-Benutzern, -Benutzergruppen oder -Rollen. Diese Richtlinien steuern, welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen identitätsbasierter Richtlinien finden Sie unter Definieren benutzerdefinierter IAM-Berechtigungen mit vom Kunden verwalteten Richtlinien im IAM-Benutzerhandbuch.

Mit identitätsbasierten IAM-Richtlinien können Sie angeben, welche Aktionen und Ressourcen zugelassen oder abgelehnt werden. Darüber hinaus können Sie die Bedingungen festlegen, unter denen Aktionen zugelassen oder abgelehnt werden. Sie können den Prinzipal nicht in einer identitätsbasierten Richtlinie angeben, da er für den Benutzer oder die Rolle gilt, dem er zugeordnet ist. Informationen zu sämtlichen Elementen, die Sie in einer JSON-Richtlinie verwenden, finden Sie in der IAM-Referenz für JSON-Richtlinienelemente im IAM-Benutzerhandbuch.

Beispiele für identitätsbasierte Richtlinien für AWS End User Messaging Social

Beispiele für identitätsbasierte Richtlinien für AWS End User Messaging Social finden Sie unter. Beispiele für identitätsbasierte Richtlinien für AWS End User Messaging Social

Ressourcenbasierte Richtlinien in AWS End User Messaging Social

Unterstützt ressourcenbasierte Richtlinien: Nein

Ressourcenbasierte Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anfügen. Beispiele für ressourcenbasierte Richtlinien sind IAM-Rollen-Vertrauensrichtlinien und Amazon-S3-Bucket-Richtlinien. In Services, die ressourcenbasierte Richtlinien unterstützen, können Service-Administratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource zu steuern. Für die Ressource, an welche die Richtlinie angehängt ist, legt die Richtlinie fest, welche Aktionen ein bestimmter Prinzipal unter welchen Bedingungen für diese Ressource ausführen kann. Sie müssen in einer ressourcenbasierten Richtlinie einen Prinzipal angeben. Zu den Prinzipalen können Konten, Benutzer, Rollen, Verbundbenutzer oder gehören. AWS-Services

Um kontoübergreifenden Zugriff zu ermöglichen, können Sie ein gesamtes Konto oder IAM-Entitäten in einem anderen Konto als Prinzipal in einer ressourcenbasierten Richtlinie angeben. Durch das Hinzufügen eines kontoübergreifenden Auftraggebers zu einer ressourcenbasierten Richtlinie ist nur die halbe Vertrauensbeziehung eingerichtet. Wenn sich der Prinzipal und die Ressource unterscheiden AWS-Konten, muss ein IAM-Administrator des vertrauenswürdigen Kontos auch der Prinzipalentität (Benutzer oder Rolle) die Berechtigung zum Zugriff auf die Ressource erteilen. Sie erteilen Berechtigungen, indem Sie der juristischen Stelle eine identitätsbasierte Richtlinie anfügen. Wenn jedoch eine ressourcenbasierte Richtlinie Zugriff auf einen Prinzipal in demselben Konto gewährt, ist keine zusätzliche identitätsbasierte Richtlinie erforderlich. Weitere Informationen finden Sie unter Kontoübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch.

Richtlinienaktionen für AWS End User Messaging Social

Unterstützt Richtlinienaktionen: Ja

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer auf was Zugriff hat. Das heißt, welcher Prinzipal Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen kann.

Das Element `Action` einer JSON-Richtlinie beschreibt die Aktionen, mit denen Sie den Zugriff in einer Richtlinie zulassen oder verweigern können. Richtlinienaktionen haben normalerweise denselben Namen wie der zugehörige AWS API-Vorgang. Es gibt einige Ausnahmen, z. B. Aktionen, die nur mit Genehmigung durchgeführt werden können und für die es keinen passenden API-Vorgang gibt. Es gibt auch einige Operationen, die mehrere Aktionen in einer Richtlinie erfordern. Diese zusätzlichen Aktionen werden als abhängige Aktionen bezeichnet.

Schließen Sie Aktionen in eine Richtlinie ein, um Berechtigungen zur Durchführung der zugeordneten Operation zu erteilen.

Eine Liste der Aktionen von AWS End User Messaging Social finden Sie in der Serviceautorisierungsreferenz unter Von AWS End User Messaging Social definierte Aktionen.

Bei Richtlinienaktionen in AWS End User Messaging Social wird vor der Aktion das folgende Präfix verwendet:

```
social-messaging
```

Um mehrere Aktionen in einer einzigen Anweisung anzugeben, trennen Sie sie mit Kommata:

```
"Action": [
      "social-messaging:action1",
      "social-messaging:action2"
         ]
```

Beispiele für identitätsbasierte Richtlinien von AWS End User Messaging Social finden Sie unter. Beispiele für identitätsbasierte Richtlinien für AWS End User Messaging Social

Richtlinienressourcen für AWS End User Messaging Social

Unterstützt Richtlinienressourcen: Ja

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer Zugriff auf was hat. Das heißt, welcher Prinzipal Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen kann.

Das JSON-Richtlinienelement `Resource` gibt die Objekte an, auf welche die Aktion angewendet wird. Anweisungen müssen entweder ein – `Resource`oder ein `NotResource`-Element enthalten. Als bewährte Methode geben Sie eine Ressource mit dem zugehörigen Amazon-Ressourcennamen (ARN) an. Sie können dies für Aktionen tun, die einen bestimmten Ressourcentyp unterstützen, der als Berechtigungen auf Ressourcenebene bezeichnet wird.

Verwenden Sie für Aktionen, die keine Berechtigungen auf Ressourcenebene unterstützen, z. B. Auflistungsoperationen, einen Platzhalter (*), um anzugeben, dass die Anweisung für alle Ressourcen gilt.

```
"Resource": "*"
```

Eine Liste der Ressourcentypen und der zugehörigen ARNs Ressourcentypen für AWS End User Messaging Social finden Sie in der Serviceautorisierungsreferenz unter Von AWS End User Messaging Social definierte Ressourcen. Informationen darüber, mit welchen Aktionen Sie den ARN jeder Ressource angeben können, finden Sie unter Von AWS End User Messaging Social definierte Aktionen.

Beispiele für identitätsbasierte Richtlinien von AWS End User Messaging Social finden Sie unter. Beispiele für identitätsbasierte Richtlinien für AWS End User Messaging Social

Bedingungsschlüssel für Richtlinien für AWS End User Messaging Social

Unterstützt servicespezifische Richtlinienbedingungsschlüssel: Ja

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer auf was Zugriff hat. Das heißt, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Das Element `Condition` (oder `Condition` block) ermöglicht Ihnen die Angabe der Bedingungen, unter denen eine Anweisung wirksam ist. Das Element `Condition` ist optional. Sie können bedingte Ausdrücke erstellen, die Bedingungsoperatoren verwenden, z. B. ist gleich oder kleiner als, damit die Bedingung in der Richtlinie mit Werten in der Anforderung übereinstimmt.

Wenn Sie mehrere `Condition`-Elemente in einer Anweisung oder mehrere Schlüssel in einem einzelnen `Condition`-Element angeben, wertet AWS diese mittels einer logischen `AND`-Operation aus. Wenn Sie mehrere Werte für einen einzelnen Bedingungsschlüssel angeben, AWS wertet die Bedingung mithilfe einer logischen `OR` Operation aus. Alle Bedingungen müssen erfüllt werden, bevor die Berechtigungen der Anweisung gewährt werden.

Sie können auch Platzhaltervariablen verwenden, wenn Sie Bedingungen angeben. Beispielsweise können Sie einem IAM-Benutzer die Berechtigung für den Zugriff auf eine Ressource nur dann gewähren, wenn sie mit dessen IAM-Benutzernamen gekennzeichnet ist. Weitere Informationen finden Sie unter IAM-Richtlinienelemente: Variablen und Tags im IAM-Benutzerhandbuch.

AWS unterstützt globale Bedingungsschlüssel und dienstspezifische Bedingungsschlüssel. Eine Übersicht aller AWS globalen Bedingungsschlüssel finden Sie unter Kontextschlüssel für AWS globale Bedingungen im IAM-Benutzerhandbuch.

Eine Liste der Bedingungsschlüssel für AWS End User Messaging Social finden Sie unter Bedingungsschlüssel für AWS End User Messaging Social in der Service Authorization Reference. Informationen zu den Aktionen und Ressourcen, mit denen Sie einen Bedingungsschlüssel verwenden können, finden Sie unter Von AWS End User Messaging Social definierte Aktionen.

Beispiele für identitätsbasierte Richtlinien von AWS End User Messaging Social finden Sie unter. Beispiele für identitätsbasierte Richtlinien für AWS End User Messaging Social

ACLs in AWS End User Messaging Social

Unterstützt ACLs: Nein

Zugriffskontrolllisten (ACLs) steuern, welche Principals (Kontomitglieder, Benutzer oder Rollen) über Zugriffsberechtigungen für eine Ressource verfügen. ACLs ähneln ressourcenbasierten Richtlinien, verwenden jedoch nicht das JSON-Richtliniendokumentformat.

ABAC mit AWS Endbenutzer-Messaging Social

Unterstützt ABAC (Tags in Richtlinien): Teilweise

Die attributbasierte Zugriffskontrolle (ABAC) ist eine Autorisierungsstrategie, bei der Berechtigungen basierend auf Attributen definiert werden. In AWS werden diese Attribute als Tags bezeichnet. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und an viele AWS Ressourcen anhängen. Das Markieren von Entitäten und Ressourcen ist der erste Schritt von ABAC. Anschließend entwerfen Sie ABAC-Richtlinien, um Operationen zuzulassen, wenn das Tag des Prinzipals mit dem Tag der Ressource übereinstimmt, auf die sie zugreifen möchten.

ABAC ist in Umgebungen hilfreich, die schnell wachsen, und unterstützt Sie in Situationen, in denen die Richtlinienverwaltung mühsam wird.

Um den Zugriff auf der Grundlage von Tags zu steuern, geben Sie im Bedingungselement einer Richtlinie Tag-Informationen an, indem Sie die Schlüssel `aws:ResourceTag/`*`key-name`*, `aws:RequestTag/`*`key-name`*, oder Bedingung `aws:TagKeys` verwenden.

Wenn ein Service alle drei Bedingungsschlüssel für jeden Ressourcentyp unterstützt, lautet der Wert für den Service Ja. Wenn ein Service alle drei Bedingungsschlüssel für nur einige Ressourcentypen unterstützt, lautet der Wert Teilweise.

Weitere Informationen zu ABAC finden Sie unter Definieren von Berechtigungen mit ABAC-Autorisierung im IAM-Benutzerhandbuch. Um ein Tutorial mit Schritten zur Einstellung von ABAC anzuzeigen, siehe Attributbasierte Zugriffskontrolle (ABAC) verwenden im IAM-Benutzerhandbuch.

Verwenden temporärer Anmeldeinformationen mit AWS End User Messaging Social

Unterstützt temporäre Anmeldeinformationen: Ja

Einige funktionieren AWS-Services nicht, wenn Sie sich mit temporären Anmeldeinformationen anmelden. Weitere Informationen, einschließlich Informationen, die mit temporären Anmeldeinformationen AWS-Services funktionieren AWS-Services , finden Sie im IAM-Benutzerhandbuch unter Diese Option funktioniert mit IAM.

Sie verwenden temporäre Anmeldeinformationen, wenn Sie sich mit einer anderen AWS Management Console Methode als einem Benutzernamen und einem Passwort anmelden. Wenn Sie beispielsweise AWS über den Single Sign-On-Link (SSO) Ihres Unternehmens darauf zugreifen, werden bei diesem Vorgang automatisch temporäre Anmeldeinformationen erstellt. Sie erstellen auch automatisch temporäre Anmeldeinformationen, wenn Sie sich als Benutzer bei der Konsole anmelden und dann die Rollen wechseln. Weitere Informationen zum Wechseln von Rollen finden Sie unter Wechseln von einer Benutzerrolle zu einer IAM-Rolle (Konsole) im IAM-Benutzerhandbuch.

Mithilfe der AWS API AWS CLI oder können Sie temporäre Anmeldeinformationen manuell erstellen. Sie können diese temporären Anmeldeinformationen dann für den Zugriff verwenden AWS. AWS empfiehlt, temporäre Anmeldeinformationen dynamisch zu generieren, anstatt langfristige Zugriffsschlüssel zu verwenden. Weitere Informationen finden Sie unter Temporäre Sicherheitsanmeldeinformationen in IAM.

Serviceübergreifende Prinzipalberechtigungen für AWS End User Messaging Social

Unterstützt Forward Access Sessions (FAS): Ja

Wenn Sie einen IAM-Benutzer oder eine IAM-Rolle verwenden, um Aktionen auszuführen AWS, gelten Sie als Principal. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service initiieren. FAS verwendet die Berechtigungen des Prinzipals, der einen aufruft AWS-Service, kombiniert mit der Anforderung, Anfragen an nachgelagerte Dienste AWS-Service zu stellen. FAS-Anfragen werden nur gestellt, wenn ein Dienst eine Anfrage erhält, für deren Abschluss Interaktionen mit anderen AWS-Services oder Ressourcen erforderlich sind. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen. Einzelheiten zu den Richtlinien für FAS-Anfragen finden Sie unter Zugriffssitzungen weiterleiten.

Servicerollen für AWS End User Messaging Social

Unterstützt Servicerollen: Ja

Eine Servicerolle ist eine IAM-Rolle, die ein Service annimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM-Administrator kann eine Servicerolle innerhalb von IAM erstellen, ändern und löschen. Weitere Informationen finden Sie unter Erstellen einer Rolle zum Delegieren von Berechtigungen an einen AWS-Service im IAM-Benutzerhandbuch.

> **Warning**
>
> Durch das Ändern der Berechtigungen für eine Servicerolle kann die Funktionalität von AWS End User Messaging Social beeinträchtigt werden. Bearbeiten Sie Servicerollen nur, wenn AWS End User Messaging Social eine Anleitung dazu bereitstellt.

Dienstbezogene Rollen für AWS End User Messaging Social

Unterstützt dienstbezogene Rollen: Ja

Eine serviceverknüpfte Rolle ist eine Art von Servicerolle, die mit einer verknüpft ist. AWS-Service Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Dienstbezogene Rollen werden in Ihrem Dienst angezeigt AWS-Konto und gehören dem Dienst. Ein IAM-Administrator kann die Berechtigungen für Service-verknüpfte Rollen anzeigen, aber nicht bearbeiten.

Details zum Erstellen oder Verwalten von serviceverknüpften Rollen finden Sie unter AWS -Services, die mit IAM funktionieren. Suchen Sie in der Tabelle nach einem Service mit einem `Yes` in der Spalte Service-linked role (Serviceverknüpfte Rolle). Wählen Sie den Link Yes (Ja) aus, um die Dokumentation für die serviceverknüpfte Rolle für diesen Service anzuzeigen.

Beispiele für identitätsbasierte Richtlinien für AWS End User Messaging Social

Standardmäßig sind Benutzer und Rollen nicht berechtigt, AWS End User Messaging Social-Ressourcen zu erstellen oder zu ändern. Sie können auch keine Aufgaben mithilfe der AWS API AWS Management Console, AWS Command Line Interface (AWS CLI) oder ausführen. Ein IAM-Administrator muss IAM-Richtlinien erstellen, die Benutzern die Berechtigung erteilen, Aktionen für die Ressourcen auszuführen, die sie benötigen. Der Administrator kann dann die IAM-Richtlinien zu Rollen hinzufügen, und Benutzer können die Rollen annehmen.

Informationen dazu, wie Sie unter Verwendung dieser beispielhaften JSON-Richtliniendokumente eine identitätsbasierte IAM-Richtlinie erstellen, finden Sie unter Erstellen von IAM-Richtlinien (Konsole) im IAM-Benutzerhandbuch.

Einzelheiten zu den von AWS End User Messaging Social definierten Aktionen und Ressourcentypen, einschließlich des Formats ARNs für die einzelnen Ressourcentypen, finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für AWS End User Messaging Social in der Referenz zur Serviceautorisierung.

Themen

- Bewährte Methoden für Richtlinien
- Verwenden der AWS End User Messaging Social-Konsole
- Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer

Bewährte Methoden für Richtlinien

Identitätsbasierte Richtlinien legen fest, ob jemand AWS End User Messaging Social-Ressourcen in Ihrem Konto erstellen, darauf zugreifen oder sie löschen kann. Dies kann zusätzliche Kosten für Ihr verursachen AWS-Konto. Befolgen Sie beim Erstellen oder Bearbeiten identitätsbasierter Richtlinien die folgenden Anleitungen und Empfehlungen:

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten — Verwenden Sie die AWS verwalteten Richtlinien, die Berechtigungen für viele gängige Anwendungsfälle gewähren, um Ihren Benutzern und Workloads zunächst Berechtigungen zu gewähren. Sie sind in Ihrem verfügbar. AWS-Konto Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie vom AWS Kunden verwaltete Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind. Weitere Informationen finden Sie unter AWS -verwaltete Richtlinien oder AWS -verwaltete Richtlinien für Auftrags-Funktionen im IAM-Benutzerhandbuch.
- Anwendung von Berechtigungen mit den geringsten Rechten – Wenn Sie mit IAM-Richtlinien Berechtigungen festlegen, gewähren Sie nur die Berechtigungen, die für die Durchführung einer Aufgabe erforderlich sind. Sie tun dies, indem Sie die Aktionen definieren, die für bestimmte Ressourcen unter bestimmten Bedingungen durchgeführt werden können, auch bekannt als die geringsten Berechtigungen. Weitere Informationen zur Verwendung von IAM zum Anwenden von Berechtigungen finden Sie unter Richtlinien und Berechtigungen in IAM im IAM-Benutzerhandbuch.

- Verwenden von Bedingungen in IAM-Richtlinien zur weiteren Einschränkung des Zugriffs – Sie können Ihren Richtlinien eine Bedingung hinzufügen, um den Zugriff auf Aktionen und Ressourcen zu beschränken. Sie können beispielsweise eine Richtlinienbedingung schreiben, um festzulegen, dass alle Anforderungen mithilfe von SSL gesendet werden müssen. Sie können auch Bedingungen verwenden, um Zugriff auf Serviceaktionen zu gewähren, wenn diese für einen bestimmten Zweck verwendet werden AWS-Service, z. AWS CloudFormation B. Weitere Informationen finden Sie unter IAM-JSON-Richtlinienelemente: Bedingung im IAM-Benutzerhandbuch.
- Verwenden von IAM Access Analyzer zur Validierung Ihrer IAM-Richtlinien, um sichere und funktionale Berechtigungen zu gewährleisten – IAM Access Analyzer validiert neue und vorhandene Richtlinien, damit die Richtlinien der IAM-Richtliniensprache (JSON) und den bewährten IAM-Methoden entsprechen. IAM Access Analyzer stellt mehr als 100 Richtlinienprüfungen und umsetzbare Empfehlungen zur Verfügung, damit Sie sichere und funktionale Richtlinien erstellen können. Weitere Informationen finden Sie unter Richtlinienvalidierung mit IAM Access Analyzer im IAM-Benutzerhandbuch.
- Multi-Faktor-Authentifizierung (MFA) erforderlich — Wenn Sie ein Szenario haben, das IAM-Benutzer oder einen Root-Benutzer in Ihrem System erfordert AWS-Konto, aktivieren Sie MFA für zusätzliche Sicherheit. Um MFA beim Aufrufen von API-Vorgängen anzufordern, fügen Sie Ihren Richtlinien MFA-Bedingungen hinzu. Weitere Informationen finden Sie unter Sicherer API-Zugriff mit MFA im IAM-Benutzerhandbuch.

Weitere Informationen zu bewährten Methoden in IAM finden Sie unter Bewährte Methoden für die Sicherheit in IAM im IAM-Benutzerhandbuch.

Verwenden der AWS End User Messaging Social-Konsole

Um auf die AWS End User Messaging Social-Konsole zugreifen zu können, benötigen Sie ein Mindestmaß an Berechtigungen. Diese Berechtigungen müssen es Ihnen ermöglichen, Details zu den AWS End User Messaging Social-Ressourcen in Ihrem aufzulisten und einzusehen AWS-Konto. Wenn Sie eine identitätsbasierte Richtlinie erstellen, die strenger ist als die mindestens erforderlichen Berechtigungen, funktioniert die Konsole nicht wie vorgesehen für Entitäten (Benutzer oder Rollen) mit dieser Richtlinie.

Sie müssen Benutzern, die nur die API AWS CLI oder die AWS API aufrufen, keine Mindestberechtigungen für die Konsole gewähren. Stattdessen sollten Sie nur Zugriff auf die Aktionen zulassen, die der API-Operation entsprechen, die die Benutzer ausführen möchten.

Um sicherzustellen, dass Benutzer und Rollen die AWS End User Messaging Social-Konsole weiterhin verwenden können, fügen Sie den Entitäten auch die AWS End User Messaging Social-*ConsoleAccess* oder *ReadOnly* AWS verwaltete Richtlinie hinzu. Weitere Informationen finden Sie unter Hinzufügen von Berechtigungen zu einem Benutzer im IAM-Benutzerhandbuch.

Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer

In diesem Beispiel wird gezeigt, wie Sie eine Richtlinie erstellen, die IAM-Benutzern die Berechtigung zum Anzeigen der eingebundenen Richtlinien und verwalteten Richtlinien gewährt, die ihrer Benutzeridentität angefügt sind. Diese Richtlinie umfasst Berechtigungen zum Ausführen dieser Aktion auf der Konsole oder programmgesteuert mithilfe der AWS CLI AWS OR-API.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
```

```
    ]
}
```

AWS verwaltete Richtlinien für AWS End User Messaging Social

Um Benutzern, Gruppen und Rollen Berechtigungen hinzuzufügen, ist es einfacher, AWS verwaltete Richtlinien zu verwenden, als Richtlinien selbst zu schreiben. Es erfordert Zeit und Fachwissen, um von Kunden verwaltete IAM-Richtlinien zu erstellen, die Ihrem Team nur die benötigten Berechtigungen bieten. Um schnell loszulegen, können Sie unsere AWS verwalteten Richtlinien verwenden. Diese Richtlinien decken allgemeine Anwendungsfälle ab und sind in Ihrem AWS-Konto verfügbar. Weitere Informationen zu AWS verwalteten Richtlinien finden Sie im IAM-Benutzerhandbuch unter AWS Verwaltete Richtlinien.

AWS Dienste verwalten und aktualisieren AWS verwaltete Richtlinien. Sie können die Berechtigungen in AWS verwalteten Richtlinien nicht ändern. Services fügen einer von AWS verwalteten Richtlinien gelegentlich zusätzliche Berechtigungen hinzu, um neue Features zu unterstützen. Diese Art von Update betrifft alle Identitäten (Benutzer, Gruppen und Rollen), an welche die Richtlinie angehängt ist. Services aktualisieren eine von AWS verwaltete Richtlinie am ehesten, ein neues Feature gestartet wird oder neue Vorgänge verfügbar werden. Dienste entfernen keine Berechtigungen aus einer AWS verwalteten Richtlinie, sodass durch Richtlinienaktualisierungen Ihre bestehenden Berechtigungen nicht beeinträchtigt werden.

AWS Unterstützt außerdem verwaltete Richtlinien für Jobfunktionen, die sich über mehrere Dienste erstrecken. Die ReadOnlyAccess AWS verwaltete Richtlinie bietet beispielsweise schreibgeschützten Zugriff auf alle AWS Dienste und Ressourcen. Wenn ein Dienst eine neue Funktion startet, werden nur Leseberechtigungen für neue Operationen und Ressourcen AWS hinzugefügt. Eine Liste und Beschreibungen der Richtlinien für Auftragsfunktionen finden Sie in Verwaltete AWS -Richtlinien für Auftragsfunktionen im IAM-Leitfaden.

AWS End User Messaging Social aktualisiert verwaltete Richtlinien AWS

Sehen Sie sich Details zu Aktualisierungen der AWS verwalteten Richtlinien für AWS End User Messaging Social an, seit dieser Dienst begonnen hat, diese Änderungen zu verfolgen. Wenn Sie automatische Benachrichtigungen über Änderungen an dieser Seite erhalten möchten, abonnieren Sie den RSS-Feed auf der Seite mit dem Verlauf von AWS End User Messaging Social Document.

Änderung	Beschreibung	Datum
AWS End User Messaging Social hat damit begonnen, Änderungen zu verfolgen	AWS End User Messaging Social hat damit begonnen, Änderungen an seinen AWS verwalteten Richtlinien nachzuverfolgen.	10. Oktober 2024

Problembehebung bei AWS Endbenutzernachrichten Soziale Identität und Zugriff

Verwenden Sie die folgenden Informationen, um häufig auftretende Probleme zu diagnostizieren und zu beheben, die bei der Arbeit mit AWS End User Messaging Social und IAM auftreten können.

Themen

- Ich bin nicht berechtigt, eine Aktion in AWS End User Messaging Social durchzuführen
- Ich bin nicht berechtigt, iam auszuführen: PassRole
- Ich möchte Personen außerhalb von mir den Zugriff AWS-Konto auf meine Social Media Ressourcen von AWS End User Messaging ermöglichen

Ich bin nicht berechtigt, eine Aktion in AWS End User Messaging Social durchzuführen

Wenn Sie eine Fehlermeldung erhalten, dass Sie nicht zur Durchführung einer Aktion berechtigt sind, müssen Ihre Richtlinien aktualisiert werden, damit Sie die Aktion durchführen können.

Der folgende Beispielfehler tritt auf, wenn der IAM-Benutzer `mateojackson` versucht, über die Konsole Details zu einer fiktiven *`my-example-widget`*-Ressource anzuzeigen, jedoch nicht über `social-messaging:`*`GetWidget`*-Berechtigungen verfügt.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform: social-
messaging:GetWidget on resource: my-example-widget
```

In diesem Fall muss die Richtlinie für den Benutzer `mateojackson` aktualisiert werden, damit er mit der `social-messaging:GetWidget`-Aktion auf die *`my-example-widget`*-Ressource zugreifen kann.

Wenn Sie Hilfe benötigen, wenden Sie sich an Ihren AWS Administrator. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

Ich bin nicht berechtigt, iam auszuführen: PassRole

Wenn Sie die Fehlermeldung erhalten, dass Sie nicht zur Durchführung der `iam:PassRole` Aktion berechtigt sind, müssen Ihre Richtlinien aktualisiert werden, damit Sie eine Rolle an AWS End User Messaging Social übergeben können.

Einige AWS-Services ermöglichen es Ihnen, eine bestehende Rolle an diesen Dienst zu übergeben, anstatt eine neue Servicerolle oder eine dienstverknüpfte Rolle zu erstellen. Hierzu benötigen Sie Berechtigungen für die Übergabe der Rolle an den Dienst.

Der folgende Beispielfehler tritt auf, wenn ein IAM-Benutzer mit dem Namen `marymajor` versucht, die Konsole zu verwenden, um eine Aktion in AWS End User Messaging Social auszuführen. Die Aktion erfordert jedoch, dass der Service über Berechtigungen verfügt, die durch eine Servicerolle gewährt werden. Mary besitzt keine Berechtigungen für die Übergabe der Rolle an den Dienst.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

In diesem Fall müssen die Richtlinien von Mary aktualisiert werden, um die Aktion `iam:PassRole` ausführen zu können.

Wenn Sie Hilfe benötigen, wenden Sie sich an Ihren AWS Administrator. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

Ich möchte Personen außerhalb von mir den Zugriff AWS-Konto auf meine Social Media Ressourcen von AWS End User Messaging ermöglichen

Sie können eine Rolle erstellen, die Benutzer in anderen Konten oder Personen außerhalb Ihrer Organisation für den Zugriff auf Ihre Ressourcen verwenden können. Sie können festlegen, wem

die Übernahme der Rolle anvertraut wird. Für Dienste, die ressourcenbasierte Richtlinien oder Zugriffskontrolllisten (ACLs) unterstützen, können Sie diese Richtlinien verwenden, um Personen Zugriff auf Ihre Ressourcen zu gewähren.

Weitere Informationen dazu finden Sie hier:

- Informationen darüber, ob AWS End User Messaging Social diese Funktionen unterstützt, finden Sie unter. So funktioniert AWS End User Messaging Social mit IAM
- Informationen dazu, wie Sie Zugriff auf Ihre Ressourcen gewähren können, AWS-Konten die Ihnen gehören, finden Sie im IAM-Benutzerhandbuch unter Gewähren des Zugriffs für einen IAM-Benutzer in einem anderen AWS-Konto , den Sie besitzen.
- Informationen dazu, wie Sie Dritten Zugriff auf Ihre Ressourcen gewähren können AWS-Konten, finden Sie AWS-Konten im IAM-Benutzerhandbuch unter Gewähren des Zugriffs für Dritte.
- Informationen dazu, wie Sie über einen Identitätsverbund Zugriff gewähren, finden Sie unter Gewähren von Zugriff für extern authentifizierte Benutzer (Identitätsverbund) im IAM-Benutzerhandbuch.
- Informationen zum Unterschied zwischen der Verwendung von Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie unter Kontoübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch.

Überprüfung der Einhaltung der Vorschriften für AWS End User Messaging Social

Informationen darüber, ob AWS-Service ein AWS-Services in den Geltungsbereich bestimmter Compliance-Programme fällt, finden Sie unter Umfang nach Compliance-Programm AWS-Services unter . Wählen Sie dort das Compliance-Programm aus, an dem Sie interessiert sind. Allgemeine Informationen finden Sie unter AWS Compliance-Programme AWS .

Sie können Prüfberichte von Drittanbietern unter herunterladen AWS Artifact. Weitere Informationen finden Sie unter Berichte herunterladen unter .

Ihre Verantwortung für die Einhaltung der Vorschriften bei der Nutzung AWS-Services hängt von der Vertraulichkeit Ihrer Daten, den Compliance-Zielen Ihres Unternehmens und den geltenden Gesetzen und Vorschriften ab. AWS stellt die folgenden Ressourcen zur Verfügung, die Sie bei der Einhaltung der Vorschriften unterstützen:

- Compliance und Governance im Bereich Sicherheit – In diesen Anleitungen für die Lösungsimplementierung werden Überlegungen zur Architektur behandelt. Außerdem werden Schritte für die Bereitstellung von Sicherheits- und Compliance-Features beschrieben.
- Referenz für berechtigte HIPAA-Services – Listet berechtigte HIPAA-Services auf. Nicht alle AWS-Services sind HIPAA-fähig.
- AWS Compliance-Ressourcen — Diese Sammlung von Arbeitsmappen und Leitfäden gilt möglicherweise für Ihre Branche und Ihren Standort.
- AWS Leitfäden zur Einhaltung von Vorschriften für Kunden — Verstehen Sie das Modell der gemeinsamen Verantwortung aus dem Blickwinkel der Einhaltung von Vorschriften. In den Leitfäden werden die bewährten Verfahren zur Sicherung zusammengefasst AWS-Services und die Leitlinien den Sicherheitskontrollen in verschiedenen Frameworks (einschließlich des National Institute of Standards and Technology (NIST), des Payment Card Industry Security Standards Council (PCI) und der International Organization for Standardization (ISO)) zugeordnet.
- Evaluierung von Ressourcen anhand von Regeln im AWS Config Entwicklerhandbuch — Der AWS Config Service bewertet, wie gut Ihre Ressourcenkonfigurationen den internen Praktiken, Branchenrichtlinien und Vorschriften entsprechen.
- AWS Security Hub— Auf diese AWS-Service Weise erhalten Sie einen umfassenden Überblick über Ihren internen Sicherheitsstatus. AWS Security Hub verwendet Sicherheitskontrollen, um Ihre AWS -Ressourcen zu bewerten und Ihre Einhaltung von Sicherheitsstandards und bewährten Methoden zu überprüfen. Die Liste der unterstützten Services und Kontrollen finden Sie in der Security-Hub-Steuerelementreferenz.
- Amazon GuardDuty — Dies AWS-Service erkennt potenzielle Bedrohungen für Ihre Workloads AWS-Konten, Container und Daten, indem es Ihre Umgebung auf verdächtige und böswillige Aktivitäten überwacht. GuardDuty kann Ihnen helfen, verschiedene Compliance-Anforderungen wie PCI DSS zu erfüllen, indem es die in bestimmten Compliance-Frameworks vorgeschriebenen Anforderungen zur Erkennung von Eindringlingen erfüllt.
- AWS Audit Manager— Auf diese AWS-Service Weise können Sie Ihre AWS Nutzung kontinuierlich überprüfen, um das Risikomanagement und die Einhaltung von Vorschriften und Industriestandards zu vereinfachen.

Resilienz bei Social Messaging für AWS Endbenutzer

Die AWS globale Infrastruktur basiert auf Availability AWS-Regionen Zones. AWS-Regionen bieten mehrere physisch getrennte und isolierte Availability Zones, die über Netzwerke mit niedriger Latenz, hohem Durchsatz und hoher Redundanz miteinander verbunden sind. Mithilfe von Availability Zones

können Sie Anwendungen und Datenbanken erstellen und ausführen, die automatisch Failover zwischen Zonen ausführen, ohne dass es zu Unterbrechungen kommt. Availability Zones sind besser verfügbar, fehlertoleranter und skalierbarer als herkömmliche Infrastrukturen mit einem oder mehreren Rechenzentren.

Weitere Informationen zu Availability Zones AWS-Regionen und Availability Zones finden Sie unter AWS Globale Infrastruktur.

Zusätzlich zur AWS globalen Infrastruktur bietet AWS End User Messaging Social mehrere Funktionen, die Sie bei der Erfüllung Ihrer Datenausfallsicherheit und Ihrer Backup-Anforderungen unterstützen.

Sicherheit der Infrastruktur in AWS End User Messaging Social

Als verwalteter Service ist AWS End User Messaging Social durch die AWS globalen Netzwerksicherheitsverfahren geschützt, die im Whitepaper Amazon Web Services: Sicherheitsprozesse im Überblick beschrieben sind.

Sie verwenden AWS veröffentlichte API-Aufrufe, um über das Netzwerk auf AWS End User Messaging Social zuzugreifen. Kunden müssen Transport Layer Security (TLS) 1.0 oder neuer unterstützen. Wir empfehlen TLS 1.2 oder neuer. Clients müssen außerdem Verschlüsselungs-Suiten mit Perfect Forward Secrecy (PFS) wie DHE (Ephemeral Diffie-Hellman) oder ECDHE (Elliptic Curve Ephemeral Diffie-Hellman) unterstützen. Die meisten modernen Systemen wie Java 7 und höher unterstützen diese Modi.

Außerdem müssen Anforderungen mit einer Zugriffsschlüssel-ID und einem geheimen Zugriffsschlüssel signiert sein, der einem IAM-Prinzipal zugeordnet ist. Alternativ können Sie mit AWS Security Token Service (AWS STS) temporäre Sicherheitsanmeldeinformationen erstellen, um die Anforderungen zu signieren.

Serviceübergreifende Confused-Deputy-Prävention

Das Confused-Deputy-Problem ist ein Sicherheitsproblem, bei dem eine juristische Stelle, die nicht über die Berechtigung zum Ausführen einer Aktion verfügt, eine privilegiertere juristische Stelle zwingen kann, die Aktion auszuführen. Ein AWS dienstübergreifender Identitätswechsel kann zu einem Problem mit dem verwirrten Stellvertreter führen. Ein dienstübergreifender Identitätswechsel kann auftreten, wenn ein Dienst (der Anruf-Dienst) einen anderen Dienst anruft (den aufgerufenen

Dienst). Der aufrufende Service kann manipuliert werden, um seine Berechtigungen zu verwenden, um Aktionen auf die Ressourcen eines anderen Kunden auszuführen, für die er sonst keine Zugriffsberechtigung haben sollte. Um dies zu verhindern, bietet AWS Tools, mit denen Sie Ihre Daten für alle Services mit Serviceprinzipalen schützen können, die Zugriff auf Ressourcen in Ihrem Konto erhalten haben.

Wir empfehlen, die Kontextschlüssel `aws:SourceArn`und die `aws:SourceAccount`globalen Bedingungsschlüssel in Ressourcenrichtlinien zu verwenden, um die Berechtigungen einzuschränken, die Social Messaging einem anderen Dienst für die Ressource gewährt. Verwenden Sie `aws:SourceArn`, wenn Sie nur eine Ressource mit dem betriebsübergreifenden Zugriff verknüpfen möchten. Verwenden Sie `aws:SourceAccount`, wenn Sie zulassen möchten, dass Ressourcen in diesem Konto mit der betriebsübergreifenden Verwendung verknüpft werden.

Der effektivste Weg, um sich vor dem Confused-Deputy-Problem zu schützen, ist die Verwendung des globalen Bedingungskontext-Schlüssels `aws:SourceArn` mit dem vollständigen ARN der Ressource. Wenn Sie den vollständigen ARN der Ressource nicht kennen oder wenn Sie mehrere Ressourcen angeben, verwenden Sie den globalen Kontextbedingungsschlüssel `aws:SourceArn` mit Platzhalterzeichen (*) für die unbekannten Teile des ARN. Beispiel, `arn:aws:social-messaging:*:`*`123456789012`*`:*`.

Wenn der `aws:SourceArn`-Wert die Konto-ID nicht enthält, z. B. einen Amazon-S3-Bucket-ARN, müssen Sie beide globale Bedingungskontextschlüssel verwenden, um Berechtigungen einzuschränken.

Der `aws:SourceArn`-Wert muss ResourceDescription lauten.

Das folgende Beispiel zeigt, wie Sie die Kontextschlüssel `aws:SourceArn` und die `aws:SourceAccount` globalen Bedingungsschlüssel in Social Messaging verwenden können, um das Problem des verwirrten Stellvertreters zu vermeiden.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Sid": "ConfusedDeputyPreventionExamplePolicy",
    "Effect": "Allow",
    "Principal": {
      "Service": "social-messaging.amazonaws.com"
    },
    "Action": "social-messaging:ActionName",
    "Resource": [
```

```
      "arn:aws:social-messaging:::ResourceName/*"
    ],
    "Condition": {
      "ArnLike": {
        "aws:SourceArn": "arn:aws:social-messaging:*:123456789012:*"
      },
      "StringEquals": {
        "aws:SourceAccount": "123456789012"
      }
    }
  }
}
```

Bewährte Methoden für die Gewährleistung der Sicherheit

AWS End User Messaging Social bietet eine Reihe von Sicherheitsfunktionen, die Sie bei der Entwicklung und Implementierung Ihrer eigenen Sicherheitsrichtlinien berücksichtigen sollten. Die folgenden bewährten Methoden sind allgemeine Richtlinien und keine vollständige Sicherheitslösung. Da diese bewährten Methoden für Ihre Umgebung möglicherweise nicht angemessen oder ausreichend sind, sollten Sie sie als hilfreiche Überlegungen und nicht als bindend ansehen.

- Erstellen Sie einen individuellen Benutzer für jede Person, die die Ressourcen von AWS End User Messaging Social verwaltet, auch für Sie. Verwenden Sie keine AWS Root-Anmeldeinformationen, um die Ressourcen von AWS End User Messaging Social zu verwalten.
- Gewähren Sie jedem Benutzer nur den Mindestsatz an Berechtigungen, die für die Ausführung seiner Aufgaben erforderlich sind.
- Verwenden Sie IAM-Gruppen, um Berechtigungen für mehrere Benutzer effektiv zu verwalten.
- Wechseln Sie regelmäßig die IAM-Anmeldeinformationen.

Verwenden von dienstbezogenen Rollen für AWS End User Messaging Social

AWS End User Messaging Social verwendet AWS Identity and Access Management dienstverknüpfte Rollen (IAM). Eine dienstverknüpfte Rolle ist eine einzigartige Art von IAM-Rolle, die direkt mit AWS End User Messaging Social verknüpft ist. Dienstbezogene Rollen sind von AWS End User Messaging Social vordefiniert und beinhalten alle Berechtigungen, die der Dienst benötigt, um andere AWS Dienste in Ihrem Namen aufzurufen.

Eine dienstbezogene Rolle erleichtert die Einrichtung von AWS End User Messaging Social, da Sie die erforderlichen Berechtigungen nicht manuell hinzufügen müssen. AWS End User Messaging Social definiert die Berechtigungen seiner dienstbezogenen Rollen. Sofern nicht anders definiert, kann nur AWS End User Messaging Social diese Rollen übernehmen. Die definierten Berechtigungen umfassen die Vertrauens- und Berechtigungsrichtlinie. Diese Berechtigungsrichtlinie kann keinen anderen IAM-Entitäten zugewiesen werden.

Sie können eine serviceverknüpfte Rolle erst löschen, nachdem ihre verwandten Ressourcen gelöscht wurden. Dadurch werden Ihre Ressourcen von AWS End User Messaging Social geschützt, da Sie nicht versehentlich die Zugriffsberechtigung für die Ressourcen entziehen können.

Informationen zu anderen Diensten, die dienstverknüpfte Rollen unterstützen, finden Sie unter AWS Dienste, die mit IAM funktionieren. Suchen Sie in der Spalte Dienstverknüpfte Rollen nach den Diensten, für die Ja steht. Wählen Sie über einen Link Ja aus, um die Dokumentation zu einer serviceverknüpften Rolle für diesen Service anzuzeigen.

Berechtigungen für dienstverknüpfte Rollen für End User Messaging Social AWS

AWS End User Messaging Social verwendet die dienstbezogene Rolle mit dem Namen AWSServiceRoleForSocialMessaging—, um Kennzahlen zu veröffentlichen und Erkenntnisse für den Versand Ihrer sozialen Nachrichten bereitzustellen.

Die AWSService RoleForSocialMessaging dienstbezogene Rolle vertraut darauf, dass die folgenden Dienste die Rolle übernehmen:

- `social-messaging.amazonaws.com`

Die genannte Rollenberechtigungsrichtlinie AWSSocial MessagingServiceRolePolicy ermöglicht es AWS End User Messaging Social, die folgenden Aktionen für die angegebenen Ressourcen durchzuführen:

- Aktion: `"cloudwatch:PutMetricData"` für `all AWS resources in the AWS/SocialMessaging namespace.`

Sie müssen Berechtigungen konfigurieren, damit eine Benutzer, Gruppen oder Rollen eine serviceverknüpfte Rolle erstellen, bearbeiten oder löschen können. Weitere Informationen finden Sie unter serviceverknüpfte Rollenberechtigung im IAM-Benutzerhandbuch.

Aktualisierungen der Richtlinie finden Sie unterAWS End User Messaging Social aktualisiert verwaltete Richtlinien AWS.

Eine dienstbezogene Rolle für AWS End User Messaging Social erstellen

Sie können die IAM-Konsole verwenden, um eine serviceverknüpfte Rolle mit dem Anwendungsfall AWSEndUserMessagingSocial — Metrics zu erstellen. Erstellen Sie in der AWS CLI oder der AWS API eine serviceverknüpfte Rolle mit dem `social-messaging.amazonaws.com` Dienstnamen. Weitere Informationen finden Sie unter Erstellen einer serviceverknüpften Rolle im IAM-Benutzerhandbuch. Wenn Sie diese serviceverknüpfte Rolle löschen, können Sie mit demselben Verfahren die Rolle erneut erstellen.

Sie können die dienstbezogene Rolle für AWS End User Messaging Social mit dem folgenden AWS CLI Befehl erstellen:

```
aws iam create-service-linked-role --aws-service-name social-messaging.amazonaws.com
```

Bearbeiten einer dienstbezogenen Rolle für AWS End User Messaging Social

AWS In End User Messaging Social können Sie die AWSService RoleForSocialMessaging dienstbezogene Rolle nicht bearbeiten. Da möglicherweise verschiedene Entitäten auf die Rolle verweisen, kann der Rollenname nach dem Erstellen einer serviceverknüpften Rolle nicht mehr geändert werden. Sie können jedoch die Beschreibung der Rolle mit IAM bearbeiten. Weitere Informationen finden Sie unter Bearbeiten einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

Löschen einer dienstbezogenen Rolle für AWS End User Messaging Social

Wenn Sie ein Feature oder einen Dienst, die bzw. der eine serviceverknüpften Rolle erfordert, nicht mehr benötigen, sollten Sie diese Rolle löschen. Auf diese Weise haben Sie keine ungenutzte juristische Stelle, die nicht aktiv überwacht oder verwaltet wird. Sie müssen jedoch die Ressourcen für Ihre serviceverknüpften Rolle zunächst bereinigen, bevor Sie sie manuell löschen können.

> **Note**
>
> Wenn der AWS End User Messaging Social-Dienst die Rolle verwendet, wenn Sie versuchen, die Ressourcen zu löschen, schlägt das Löschen möglicherweise fehl. Wenn dies passiert, warten Sie einige Minuten und versuchen Sie es erneut.

Um die Ressourcen von AWS End User Messaging Social zu entfernen, die von AWSService RoleForSocialMessaging

1. Rufen Sie die `list-linked-whatsapp-business-accounts` API auf, um zu sehen, über welche Ressourcen Sie verfügen.
2. Rufen Sie für jedes verknüpfte Whats App Business-Konto die `disassociate-whatsapp-business-account` API auf, um die Ressource aus dem SocialMessaging Dienst zu entfernen.
3. Stellen Sie sicher, dass keine Ressourcen zurückgegeben werden, indem Sie die `list-linked-whatsapp-business-accounts` API erneut aufrufen.

So löschen Sie die serviceverknüpfte Rolle mit IAM

Verwenden Sie die IAM-Konsole, die oder die AWS API AWS CLI, um die AWSService RoleForSocialMessaging serviceverknüpfte Rolle zu löschen. Weitere Informationen finden Sie unter Löschen einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

Unterstützte Regionen für Rollen, die mit dem Dienst „ AWS End User Messaging Social“ verknüpft sind

AWS End User Messaging Social unterstützt die Verwendung von dienstbezogenen Rollen in allen Regionen, in denen der Dienst verfügbar ist. Weitere Informationen finden Sie unter AWS Regionen und Endpunkte.

Greifen Sie über einen Schnittstellenendpunkt auf AWS End User Messaging Social zu (AWS PrivateLink)

Sie können AWS PrivateLink es verwenden, um eine private Verbindung zwischen Ihrer VPC und AWS End User Messaging Social herzustellen. Sie können auf AWS End User Messaging Social wie in Ihrer VPC zugreifen, ohne ein Internet-Gateway, ein NAT-Gerät, eine VPN-Verbindung oder AWS Direct Connect eine Verbindung verwenden zu müssen. Instances in Ihrer VPC benötigen keine öffentlichen IP-Adressen, um auf AWS End User Messaging Social zuzugreifen.

Sie stellen diese private Verbindung her, indem Sie einen Schnittstellen-Endpunkt erstellen, der von AWS PrivateLink unterstützt wird. Wir erstellen eine Endpunkt-Netzwerkschnittstelle in jedem Subnetz, das Sie für den Schnittstellen-Endpunkt aktivieren. Dabei handelt es sich um vom Anforderer verwaltete Netzwerkschnittstellen, die als Einstiegspunkt für den Datenverkehr dienen, der für AWS End User Messaging Social bestimmt ist.

Weitere Informationen finden Sie AWS PrivateLink im Handbuch unter Access AWS-Services through.AWS PrivateLink

Überlegungen zu AWS End User Messaging Social

Bevor Sie einen Schnittstellenendpunkt für AWS End User Messaging Social einrichten, lesen Sie die Überlegungen im AWS PrivateLink Handbuch durch.

AWS End User Messaging Social unterstützt Aufrufe aller API-Aktionen über den Endpunkt der Benutzeroberfläche.

VPC-Endpunktrichtlinien werden für AWS End User Messaging Social nicht unterstützt. Standardmäßig ist der vollständige Zugriff auf AWS End User Messaging Social über den Schnittstellenendpunkt zulässig. Alternativ können Sie den Endpunkt-Netzwerkschnittstellen eine Sicherheitsgruppe zuordnen, um den Datenverkehr zu AWS End User Messaging Social über den Schnittstellenendpunkt zu steuern.

Erstellen Sie einen Schnittstellenendpunkt für AWS End User Messaging Social

Sie können einen Schnittstellenendpunkt für AWS End User Messaging Social entweder mit der Amazon VPC-Konsole oder mit AWS Command Line Interface (AWS CLI) erstellen. Weitere

Informationen finden Sie unter Erstellen eines Schnittstellenendpunkts im AWS PrivateLink -Leitfaden.

Erstellen Sie einen Schnittstellenendpunkt für AWS End User Messaging Social mit dem folgenden Servicenamen:

- `com.amazonaws.region.social-messaging`

Wenn Sie privates DNS für den Schnittstellenendpunkt aktivieren, können Sie API-Anfragen an AWS End User Messaging Social stellen, indem Sie den standardmäßigen regionalen DNS-Namen verwenden. Beispiel, `service-name.us-east-1.amazonaws.com`.

Erstellen einer Endpunktrichtlinie für Ihren Schnittstellen-Endpunkt

Eine Endpunktrichtlinie ist eine IAM-Ressource, die Sie an einen Schnittstellen-Endpunkt anfügen können. Die standardmäßige Endpunktrichtlinie ermöglicht den vollen Zugriff auf AWS End User Messaging Social über den Schnittstellenendpunkt. Um den Zugriff auf AWS End User Messaging Social von Ihrer VPC aus zu kontrollieren, fügen Sie dem Schnittstellenendpunkt eine benutzerdefinierte Endpunktrichtlinie hinzu.

Eine Endpunktrichtlinie gibt die folgenden Informationen an:

- Die Prinzipale, die Aktionen ausführen können (AWS-Konten, IAM-Benutzer und IAM-Rollen).
- Aktionen, die ausgeführt werden können
- Die Ressourcen, auf denen die Aktionen ausgeführt werden können.

Weitere Informationen finden Sie unter Steuern des Zugriffs auf Services mit Endpunktrichtlinien im AWS PrivateLink -Leitfaden.

Beispiel: VPC-Endpunktrichtlinie für Social Media-Aktionen von AWS End User Messaging

Im Folgenden finden Sie ein Beispiel für eine benutzerdefinierte Endpunktrichtlinie. Wenn Sie diese Richtlinie an Ihren Schnittstellenendpunkt anhängen, gewährt sie allen Prinzipalen auf allen Ressourcen Zugriff auf die aufgelisteten Social Media-Aktionen von AWS End User Messaging.

```
{
   "Statement": [
```

```
      {
         "Principal": "*",
         "Effect": "Allow",
         "Action": [
            "social-messaging:DeleteWhatsAppMessageMedia",
            "social-messaging:PostWhatsAppMessageMedia",
            "social-messaging:SendWhatsAppMessage"
         ],
         "Resource":"*"
      }
   ]
}
```

Kontingente für AWS Endbenutzer-Messaging Social

Das AWS-Konto verfügt über Standardkontingente (früher als Limits bezeichnet) für jeden AWS-Service. Wenn nicht anders angegeben, gilt jedes Kontingent spezifisch für eine Region. Sie können Erhöhungen für einige Kontingente beantragen und andere Kontingente können nicht erhöht werden.

Ihr AWS-Konto hat die folgenden Kontingente für AWS End User Messaging Social.

Ressource	Standard
WhatsApp Geschäftskonto (WABA)	25 pro Region

AWS End User Messaging Social implementiert Kontingente, die die Anzahl der Anfragen einschränken, die Sie von Ihrem aus an die AWS End User Messaging Social API richten können AWS-Konto.

Operation	Standardkontingentrate (Anforderungen pro Sekunde)
SendWhatsAppMessage	1.000
PostWhatsAppMessageMedia	100
GetWhatsAppMessageMedia	100
DeleteWhatsAppMessageMedia	100
DisassociateWhatsAppBusinessAccount	10
ListWhatsAppBusinessAccount	10
TagResource	10
UntagResourceRate	10
ListTagsForResourceRate	10

Dokumentenverlauf für das AWS End User Messaging Social User Guide

In der folgenden Tabelle werden die Dokumentationsversionen für AWS End User Messaging Social beschrieben.

Änderung	Beschreibung	Datum
Neue API zum Erstellen von WhatsApp Nachrichtenvorlagen	Unterstützung für die Erstellung von WhatsApp Nachrichtenvorlagen mithilfe der AWS End User Messaging Social API wurde hinzugefügt. Weitere Informationen finden Sie unter Nachrichtenvorlagen mit der CreateWhatsAppMessageTemplate API erstellen.	25. Juli 2025
Wird pro Nachricht berechnet	Ab dem 1. Juli 2025 berechnet AWS End User Messaging Social WhatsApp Nachrichten pro Nachricht statt pro Konversation. Weitere Informationen finden Sie unter Abrechnung pro Nachricht.	30. Juni 2025
Regionale Verfügbarkeit	Unterstützung für die Region Europa (Frankfurt) hinzugefügt. Weitere Informationen finden Sie unter Regionale Verfügbarkeit.	5. Dezember 2024
Fügen Sie eine Nachricht und ein Ziel für ein Ereignis hinzu	Unterstützung für Amazon Connect als Eventziel hinzugefügt. Weitere Informationen finden Sie unter	01. Dezember 2024

	Hinzufügen einer Nachricht und eines Veranstaltungsziels.	
AWS PrivateLink	Unterstützung für hinzugefügt AWS PrivateLink. Weitere Informationen finden Sie unter AWS PrivateLink.	22. Oktober 2024
Erstversion	Erste Version des Social User Guide für AWS Endbenutzer Messaging	10. Oktober 2024

Die vorliegende Übersetzung wurde maschinell erstellt. Im Falle eines Konflikts oder eines Widerspruchs zwischen dieser übersetzten Fassung und der englischen Fassung (einschließlich infolge von Verzögerungen bei der Übersetzung) ist die englische Fassung maßgeblich.