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 umfangreichen Messaging-Funktionen und ermöglicht die Erstellung von markenspezifischen, interaktiven Inhalten mit Bildern, Videos und Schaltflächen. Mit diesem Service können Sie Ihren Anwendungen neben bestehenden Kanälen wie SMS Push-Benachrichtigungen auch WhatsApp Messaging-Funktionen hinzufügen, sodass Sie mit Kunden über ihren bevorzugten Kommunikationskanal in Kontakt treten können.

Zu Beginn können Sie entweder mithilfe des selbstgesteuerten Onboarding-Prozesses in der Social Console von AWS End User Messaging ein neues WhatsApp Geschäftskonto (WABA) erstellen oder ein vorhandenes Konto mit WABA dem Service verknüpfen.

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, dass Sie zunächst die folgenden Abschnitte 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 grundlegenden Features und Funktionen:

- 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 gesendeten Nachrichten wiederverwenden möchten.
- Zugriff auf neue umfangreiche Messaging-Funktionen für ein noch 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 MessagingSMS, um Nachrichten zu senden SMS
- 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

Interagiere mit AWS -Services über Befehle in deiner Befehlszeilen-Shell. Die AWS Command Line Interface wird unter Windows, macOS und Linux unterstützt. Weitere Informationen zu finden Sie im AWS CLIAWS Command Line Interface Benutzerhandbuch. Sie finden die AWS SMS Befehle in der AWS CLI Befehlsreferenz.

AWS SDKs

Wenn Sie es vorziehen, Anwendungen mithilfe sprachspezifischer zu erstellen, APIs anstatt eine Anfrage über HTTP oder zu übermittelnHTTPS, AWS stellt Bibliotheken, Beispiel-Code, Tutorials und andere Ressourcen bereit. Diese Bibliotheken bieten grundlegende Funktionen

zur Automatisierung von Aufgaben, z. B. kryptografisches Signieren von Anfragen, Wiederholen von Anfragen und Behandlung von Fehlermeldungen. Diese Funktionen helfen Ihnen dabei, den Einstieg effizienter zu gestalten. Weitere Informationen finden Sie unter Tools für 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 sehr 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 APIVersion
USA Ost (Nord-Virginia)	us-east-1	social-messaging.us-east-1.amazonaws.com social-messaging-fips.us-east-1.api.aws social-messaging.us-east-1.api.aws	Version 20 und höher
USA Ost (Ohio)	us-east-2	social-messaging.us-east-2.amazonaws.com	Version 20 und höher

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

Name der Region	Region	Endpunkt	WhatsApp APIVersion
Europa (London)	eu-west-2	social-messaging.eu-west-2.amazonaws.com social-messaging.eu-west-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 abschließen.

Themen

Registrieren Sie sich für eine AWS-Konto

Wenn Sie kein haben AWS-Konto, führen Sie die folgenden Schritte zum Erstellen durch.

Sich für ein () registrieren AWS-Konto

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

   Bei der Anmeldung müssen Sie auch einen Telefonanruf entgegennehmen und einen Verifizierungscode über die Telefontasten eingeben.

   Wenn Sie sich für eine anmelden AWS-Konto, Root-Benutzer des AWS-Kontoswird eine erstellt. 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 eine Bestätigungs-E-Mail, sobald die Registrierung abgeschlossen ist. Sie können jederzeit Ihre aktuelle Kontoaktivität anzeigen und Ihr Konto verwalten. Rufen Sie dazu auf https://aws.amazon.com/und klicken Sie auf My Account (Mein Konto).

Erstellen eines Benutzers mit Administratorzugriff

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

Sichern Sie Ihre Root-Benutzer des AWS-Kontos

1. Melden Sie sich bei der AWS Management Consoleals Kontoinhaber an, indem Sie Root user (Stammbenutzer) auswählen und die AWS-Konto E-Mail-Adresse Ihres 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 im Benutzerhandbuch unter Aktivieren eines virtuellen MFA Geräts für Ihren AWS-Konto IAM Root-Benutzer (Konsole).

Erstellen eines Benutzers mit Administratorzugriff

1. Aktivieren Sie 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 unter Benutzerzugriff mit der Standardeinstellung konfigurieren IAM-Identity-Center-Verzeichnis im AWS IAM Identity Center Benutzerhandbuch.

Anmelden als Administratorbenutzer

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

Hilfestellung zur Anmeldung mit einem IAM Identity-Center-Benutzer finden Sie unter Anmelden beim AWS -Zugangsportal im AWS-Anmeldung Benutzerhandbuch zu.

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

Registrieren bei WhatsApp

Ein WhatsApp Geschäftskonto (WABA) ermöglicht es Ihrem Unternehmen, die WhatsApp Geschäftsplattform zu verwenden, um Nachrichten direkt an Ihre Kunden zu senden. Sie alle WABAs sind Teil Ihres Meta-Geschäftsportfolios. A 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.

Informationen zu Ihren ersten Schritten mit AWS End User Messaging Social sind in diesem Abschnitt beschrieben. Verwenden Sie den eingebetteten Anmeldevorgang, 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 WhatsApp einrichten.
- Sie müssen ein Business Manager-Konto bei Meta erstellen und es mit Ihrem verknüpfenWABA.
- Sie müssen uns die Kontrolle über Ihr WABA Konto geben. Auf Ihren Wunsch hin werden wir Ihnen die Kontrolle über Ihren WABA Rücken in angemessener und zeitnaher Weise übertragen, indem wir die Methoden verwenden, die Meta uns zur Verfügung stellt.
- Im Zusammenhang mit Ihrer Nutzung der WhatsApp Business Solution werden Sie keine Inhalte, Informationen oder Daten einreichen, die gemäß den geltenden Gesetzen und/oder Vorschriften Schutzmaßnahmen und/oder Vertriebsbeschränkungen unterliegen.
- 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 bei der Registrierung 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 einen Einmalpasscode SMS oder einen Sprachcode (OTP) erhalten 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 SMSMMS, und Sprachnachrichten verwendet werden.
- Wenn Sie eine bestehende Datei importierenWABA, benötigen Sie die PINs für alle Telefonnummern, die mit der importierten Nummer verknüpft sindWABA. Um eine verloren gegangene oder vergessene Nummer zurückzusetzenPIN, folgen Sie den Anweisungen unter Aktualisieren PIN in der WhatsApp Business Platform API Cloud-Referenz.

Melden Sie sich über die Konsole an

Folgen Sie diesen Anweisungen, um ein neues WhatsApp Konto zu erstellen, Ihr bestehendes Konto zu migrieren oder einem bestehenden Konto eine Telefonnummer hinzuzufügenWABA. 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). Außerdem gestatten Sie AWS End User Messaging Social, 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 den Namen URL für die Website Ihres Unternehmens ein. Falls Ihr Unternehmen keine Website hat, geben Sie den Link URL zu Ihrer Social-Media-Seite ein.

   d. Wählen Sie unter Land das Land aus, in dem sich Ihr Unternehmen befindet.

   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. Es wird empfohlen, Ihren Firmennamen als Anzeigenamen zu 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 Ihr Anzeigename abgelehnt wird, wird Ihr Nachrichtenlimit pro Tag herabgesetzt und Sie könnten von WhatsApp der Verbindung getrennt werden.

      > **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 die Kategorie, die Sie sind, als Teil Ihrer Kontaktinformationen einsehen.
    - Geben Sie im Feld Unternehmensbeschreibung (Beschreibung) eine Beschreibung für Ihr Unternehmen ein. Kunden können Ihre Unternehmensbeschreibung als Teil Ihrer Kontaktinformationen einsehen.
    - Geben Sie im Feld 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 Werte-Paare, 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 zu aktivierenSNS, 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 SNS Amazon-Standardthema und geben Sie einen Namen in das Feld Themenname ein, oder wählen Sie Bestehendes SNS Amazon-Standardthema und wählen Sie ein Thema aus der Dropdownliste Thema arn aus.
17. Unter Telefonnummern:

    Für jede Telefonnummer unter WhtsApp Telefonnummern:

a. Geben Sie zur Bestätigung der Telefonnummer den vorhandenen PIN oder einen neuen PIN Code ein. Um einen verlorenen oder vergessenen PIN Code zurückzusetzen, folgen Sie den Anweisungen unter Aktualisieren PIN in der WhatsApp Business Platform API Cloud-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 APIlokaler Cloud-Speicher in der WhatsApp Business Platform Cloud API Reference.

   ii. Tags sind Schlüssel- und Werte-Paare, 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 in Amazon zu aktivierenSNS, 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**
>
> 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. Wählen Sie für Amazon SNS entweder Neues SNS Amazon-Standardthema und geben Sie einen Namen in das Feld Themenname ein, oder wählen Sie Bestehendes SNS Amazon-Standardthema und wählen Sie ein Thema aus der Dropdownliste Thema arn aus.

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

Nächste Schritte

Sobald Sie sich angemeldet haben, können Sie Nachrichten senden. Wenn Sie bereit sind, Nachrichten in großem Umfang zu senden, führen Sie die Unternehmensverifizierung durch. 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

Ein WhatsApp Geschäftskonto (WABA) ermöglicht es Ihrem Unternehmen, die WhatsApp Geschäftsplattform zu 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 einer existieren AWS-Region. Weitere Informationen zu WhatsApp Geschäftskonten finden Sie unter WhatsAppGeschäftskonten in der WhatsApp Business Platform API Cloud-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 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 WhatsApp einrichten.
- Sie müssen ein Business Manager-Konto bei Meta erstellen und es mit Ihrem verknüpfenWABA.
- Sie müssen uns die Kontrolle über WABA Sie geben. Auf Ihren Wunsch hin werden wir Ihnen die Kontrolle über Ihren WABA Rücken in angemessener und zeitnaher Weise übertragen, indem wir die Methoden verwenden, die Meta uns zur Verfügung stellt.
- Im Zusammenhang mit Ihrer Nutzung der WhatsApp Business Solution werden Sie keine Inhalte, Informationen oder Daten einreichen, die gemäß den geltenden Gesetzen und/oder Vorschriften Schutzmaßnahmen und/oder Vertriebsbeschränkungen unterliegen.
- WhatsAppDie Preise für die Nutzung der WhatsApp Business Solution finden Sie unter https://developers.facebook.com/docs/whatsapp/pricing.

Themen

Ein WhatsApp Geschäftskonto (WABA) in AWS End User Messaging Social anzeigen

Folgen Sie diesen Anweisungen, um die mit Ihnen WABA verknüpften Seiten einzusehen AWS-Konto.

1. Öffnen Sie die AWS End User Messaging Social-Konsole unter https://console.aws.amazon.com/social-messaging/.
2. Wählen Sie unter Geschäftskonten eine ausWABA.
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 der Registerkarte Vorlagen die Option Nachrichtenvorlagen verwalten aus, um Ihre WhatsApp Vorlagen über Meta zu bearbeiten. Jede Vorlage 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 ein neues WABA hinzu, wenn Sie bereits ein WhatsApp Unternehmensprofil haben. Im Rahmen der Erstellung eines neuen müssen WABA Sie dem eine Telefonnummer hinzufügenWABA.

- Gehen Sie wie folgt vorWABA, um Ihrem Konto eine neue hinzuzufügenErste 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 verfügt über zwei Arten von Geschäftskonten:

- Geschäftskonto: WhatsApp überprüft die Echtheit jedes Kontos auf der WhatsApp Geschäftsplattform. Wenn ein Geschäftskonto den Geschäftsverifizierungsprozess abgeschlossen hat, ist der Name des Unternehmens für Benutzer sichtbar, auch wenn sie das Unternehmen nicht zu ihrem Adressbuch hinzugefügt haben. Diese Funktion hilft Benutzern dabei, verifizierte Geschäftskonten zu identifizieren WhatsApp.
- Offizielles Geschäftskonto: Neben den Vorteilen eines Geschäftskontos verfügt ein offizielles Geschäftskonto über ein grünes Häkchen in seinem Profil und in den Kopfzeilen des Chat-Threads.

  Für die Genehmigung eines WhatsApp offiziellen Geschäftskontos (OBA) ist der Nachweis erforderlich, dass das Unternehmen bekannt ist und von den Verbrauchern anerkannt wird, z. B. durch Artikel, Blogbeiträge oder unabhängige 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 dies beantragen, WhatsApp OBA müssen ihren Ruf und ihre Anerkennung nachweisen, aber die endgültige Genehmigung liegt 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 nur 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 API Cloud-Referenz.
- Weitere Informationen zum Prozess der Unternehmensverifizierung finden Sie unter Unternehmensverifizierung in der WhatsApp Business Platform API Cloud-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 bei der Verwendung mit einem WhatsApp Geschäftskonto

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

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

Sie können eine SMS -fähige Telefonnummer über AWS End User Messaging erhalten, SMS indem Sie wie folgt vorgehen:

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

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

Hinzufügen einer Telefonnummer zu einem WhatsApp Geschäftskonto (WABA)

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

Voraussetzungen

Bevor Sie beginnen, müssen die folgenden Voraussetzungen erfüllt sein:

- Die Telefonnummer muss in der Lage sein, entweder einen Einmalpasscode SMS oder einen Sprachcode (OTP) zu empfangen. Dies ist die Telefonnummer, die zu Ihrer WABA hinzugefügt wurde.
- Die Telefonnummer darf keiner anderen zugeordnet seinWABA.

Hinzufügen einer Telefonnummer WABA

Um eine neue Telefonnummer zu Ihrer bestehenden hinzuzufügen WABA

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 das WABA und das WhatsApp Unternehmensprofil, zu dem 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 WhtsApp Telefonnummern:

    a. Geben Sie zur Bestätigung der Telefonnummer den vorhandenen PIN oder einen neuen PIN Code ein. Um einen verlorenen oder vergessenen PIN Code zurückzusetzen, folgen Sie den Anweisungen unter Aktualisieren PIN in der WhatsApp Business Platform API Cloud-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 APIlokaler Cloud-Speicher in der WhatsAppBusiness Platform Cloud API Reference.

        ii. Tags sind Schlüssel- und Werte-Paare, 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 in Amazon zu aktivierenSNS, einschließlich der Protokollierung des Empfangs einer Kundennachricht, aktivieren Sie das Veröffentlichen von Nachrichten und Ereignissen. 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. Wählen Sie für Amazon SNS entweder Neues SNS Amazon-Standardthema und geben Sie einen Namen in das Feld Themenname ein, oder wählen Sie Bestehendes SNS Amazon-Standardthema und wählen Sie ein Thema aus der Dropdownliste Thema arn aus.

13. 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 lauten.

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 Abschnitt Telefonnummern eine Telefonnummer.
4. Der Abschnitt mit den Telefonnummerdetails enthält die Rufnummer-ID der Telefonnummer.

Erhöhen Sie die Beschränkungen für Messaging-Konversationen WhatsApp

Die Nachrichtenlimits beziehen sich auf die maximale Anzahl von geschäftlich initiierten Konversationen, die eine geschäftliche Telefonnummer in einem 24-Stunden-Zeitraum öffnen 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 eine Zahl MPS von 80. Meta kann deinen Wert MPS auf 1.000 erhöhen, wenn die folgenden Bedingungen erfüllt sind:

- 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 7 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 Telefonnummernstatus

- Verbunden: Sie können innerhalb Ihres Nachrichtenlimits Nachrichten senden.
- Markiert: Die Qualität Ihrer Telefonnummer ist gering und muss verbessert werden. Wenn sich Ihre Telefonqualität innerhalb von 7 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, können aber weiterhin auf eingehende Kundennachrichten antworten. Sobald der Zeitraum von 24 Stunden abgelaufen ist, 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 eine ausWABA.
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

Sie können Nachrichtenvorlagen für Nachrichtentypen verwenden, 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 WhatsApp diesem überprüft.

Sie können die folgenden Vorlagentypen versenden:

- Textbasiert
- Medienbasiert
- Interaktives Nachricht
- Ortsbezogene
- 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 API Cloud-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 einWABA.
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.

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 in WhatsApp

Das Template Pacing ist eine von Meta verwendete Methode, die Zeit für frühzeitiges Kundenfeedback 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 API Cloud-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 einWABA.
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 API Cloud-Referenz.

Vorlagenstatus	Bewertung der Qualität	Bedeutung
Wird überprüft		Die Nachrichtenvorlage wird überprüft. Dieser 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

Vorlagenstatus	Bewertung der Qualität	Bedeutung
		envorlagen mit diesem 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.
Beschwerde angefordert		Es wurde Berufung beantragt.

Gründe, warum eine Vorlage abgelehnt wird in 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 API Cloud-Referenz.

Nachrichten- und Ereignisziele in AWS End User Messaging Social

Ein Veranstaltungsziel ist ein SNS Amazon-Thema, an das WhatsApp Ereignisse gesendet werden. Wenn Sie die Veröffentlichung von Veranstaltungen zu einem SNS Amazon-Thema aktivieren, werden alle Ihre Sende- und Empfangsereignisse an das SNS Amazon-Thema gesendet. Verwenden Sie Ereignisse, um den Status ausgehender Nachrichten und eingehender Kundenmitteilungen 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 SNS Amazon-Thema gesendet. Dazu gehören Ereignisse für jede Telefonnummer, die einem WhatsApp Geschäftskonto zugeordnet ist. Sie WABA können ein SNS Amazon-Thema damit verknüpfen.

Voraussetzungen

Bevor Sie beginnen, sollten die folgenden Voraussetzungen erfüllt sein.

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

Fügen Sie eine Nachricht und ein Ziel für das 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 einWABA.
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. Um Ihre Veranstaltungen an ein neues SNS Amazon-Ziel zu senden, wählen Sie Neues SNS Standthema und geben Sie im Feld Themenname einen Namen ein. Das SNS Amazon-Thema wird mit Berechtigungen erstellt, die es AWS End User Messaging Social ermöglichen, auf das Thema zuzugreifen.

   Um Ihre Veranstaltungen an ein vorhandenes SNS Amazon-Ziel zu senden, wählen Sie SNSExistierendes Standardthema und anschließend ein Thema aus Topic arn. Sie müssen die folgenden Berechtigungen für das SNS Amazon-Thema anwenden:

   ```
   {
       "Effect": "Allow",
       "Principal": {
           "Service": [
             "social-messaging.amazonaws.com"
           ]
          },
       "Action": "sns:Publish",
       "Resource": "arn:{PARTITION}:sns:{REGION}:{ACCOUNT}:{TOPIC_NAME}"
   }
   ```
6. Wählen Sie Änderungen speichern.

SNSThemenrichtlinien für verschlüsselte Amazon-Themen

Sie können SNS Amazon-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 SNS Amazon-Themen mithilfe von AWS KMS Schlüsseln finden Sie unter Ermöglichen der Kompatibilität zwischen Ereignisquellen aus AWS -Services und verschlüsselten Themen im Entwicklerhandbuch für Amazon Simple Notification Service.

In der Beispielanweisung werden die optionalen, aber empfohlenen `SourceArn` -Bedingungen verwendet, `SourceAccount` um das Problem des verwirrten Stellvertreters zu vermeiden, und nur das Eigentümerkonto für AWS Endbenutzer Messaging Social hat Zugriff. Weitere Informationen zum Problem mit dem verwirrten Stellvertreter finden Sie im IAMBenutzerhandbuch unter Das Problem des verwirrten Stellvertreters.

Der verwendete Schlüssel muss symmetrisch sein. Verschlüsselte SNS Amazon-Themen unterstützen keine asymmetrischen AWS KMS -Schlüssel.

Die Schlüsselrichtlinie muss geändert werden, damit AWS Endbenutzer 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}:*"
        }
     }
}
```

Nächste Schritte

Sobald Sie Ihr SNS Amazon-Thema eingerichtet haben, müssen Sie einen Endpunkt für das Thema abonnieren. Der Endpunkt beginnt, für das zugehörige Thema veröffentlichte Nachrichten zu empfangen. Weitere Informationen zum Abonnieren eines Themas finden Sie unter Abonnieren eines SNS Amazon-Themas im Amazon SNS Developer Guide.

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 JSON WhatsApp Benachrichtigungen finden Sie in der WhatsApp Business Platform Cloud Reference unter Webhooks Notification Payload Reference und Message Status. API

AWS Nachrichtenübermittlung an Endbenutzer in sozialen Netzwerken — Header

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

```
{
  "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"
    }
  ]
}
{
//WhatsApp notification payload
}
```

Für das obige Beispielereignis gilt:

- *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.

Beispiel WhatsApp JSON für den Empfang einer Textnachricht

Im Folgenden wird der Ereignisdatensatz für eine eingehende Textnachricht von angezeigt WhatsApp. Das JSON wird generiert von WhatsApp. Eine Liste der Felder und ihrer Bedeutung finden Sie unter Webhooks Notification Payload Reference in der WhatsApp Business Platform Cloud API Reference.

```
{
//AWS End User Messaging Social header
}
{
  "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": "1723506035",
            "text": {
              "body": "Hi"
            },
            "type": "text"
```

```
          }
        ]
      },
      "field": "messages"
    }
  ]
}
```

Beispiel WhatsApp JSON 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
}
{
  "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.

Nachrichtenstatus

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 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.

Name des Status	Beschreibung
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 API Cloud-Referenz.

Mediendateien hochladen, mit denen gesendet werden soll WhatsApp

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

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

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

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

Beim vorhergehenden Befehl:

- Ersetzen *us-east-1* mit dem AWS-Region , in dem Sie WABA sich befinden.
- Ersetzen *BucketName* durch den Namen des neuen Buckets.

Um eine Datei in den Amazon-S3-Bucket zu kopieren, verwenden Sie den AWS CLI Befehl cp. Geben Sie in der Befehlszeile folgenden Befehl ein:

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

Beim vorhergehenden Befehl:

- Ersetzen *SourceFilePathAndName* durch den Dateipfad und den Namen der zu kopierenden Datei.
- Ersetzen *BucketName* durch den Namen des Buckets.

- Ersetzen *FileName* mit dem Namen, der für die Datei verwendet werden soll.

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

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

Um ein vorsigniertes zu erstellenURL, ersetzen Sie das *user input placeholders* durch Ihre eigenen Informationen.

```
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 zurückgesandten URL werden sein: `https://amzn-s3-demo-bucket1.s3.af-south-1.amazonaws.com/mydoc.txt?{Headers}`

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 API Cloud-Referenz.

Mediendateitypen

Audioformate

Audio-Typ	Erweiterung	MIMETyp	Max size
AAC	.aac	Audio/AAC	16 MB
AMR	.amr	Audio/AMR	16 MB
MP3	.mp3	Audio/MPEG	16 MB
MP4Audio	.m4a	Audio/MP4	16 MB
OGGAudio	.ogg	Audio/ogg	16 MB

Formate der Dokumente

Dokumenttyp	Erweiterung	MIMETyp	Max size
Text	.text	text/plain	100 MB
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

Image Type (Bild)	Erweiterung	MIMETyp	Max size
JPEG	JPEG	image/jpeg	5 MB
PNG	.png	image/png	5 MB

Aufkleber-Formate

Aufkleber-Typ	Erweiterung	MIMETyp	Max size
Animierter Aufkleber	.webp	image/webp	500 KB
Statischer Aufkleber	.webp	image/webp	100 KB

Videoformate

Video-Typ	Erweiterung	MIMETyp	Max size
3 GPP	. 3 gp	Video/3GP	16 MB
MP4Video	.mp4	Video/MP4	16 MB

WhatsApp Nachrichtentypen

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

Meldungstyps	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 einer Vorlagennachricht
Ort	Senden eines Speicherorts
Kontakte	Senden Sie eine Kontaktkarte
Interactive	Senden einer interaktiven Message

Weitere Ressourcen

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

Senden von Nachrichten WhatsApp mit AWS End User Messaging Social

Bevor Sie eine Nachricht senden können, müssen Sie Ihre Einstellungen abgeschlossen haben WABA und Ihr Benutzer muss sich für den Empfang von Nachrichten von Ihnen angemeldet haben, siehe. 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 an einen Benutzer gesendet werden, wenn zwischen Ihnen und dem Benutzer ein Kundendienstfenster geöffnet ist. Vorlagennachrichten können jederzeit an einen Benutzer gesendet werden, sofern der Benutzer dem Empfang von Nachrichten von Ihnen zugestimmt hat.

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

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

Themen

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

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

```
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:

- Ersetzen *{PHONE_NUMBER}* durch die Telefonnummer Ihrer Kunden.
- Ersetzen *{ORIGINATION_PHONE_NUMBER_ID}* mit der ID Ihrer Telefonnummer.

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

Im folgenden Beispiel wird gezeigt, wie Sie Ihrem Kunden mithilfe des Senden einer Mediennachricht 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 mit unterstützten Mediendateitypen finden Sie unterUnterstützte Mediendateitypen und -größen in WhatsApp.

1. Laden Sie die Mediendatei zu einem Amazon S3 S3-Bucket hoch, siheMediendateien hochladen, mit denen gesendet werden soll WhatsApp.
2. Laden Sie die Mediendatei WhatsApp mithilfe des post-whatsapp-message-mediaBefehls hoch. Bei erfolgreichem Abschluss gibt der Befehl Folgendes zurück *{MEDIA_ID}* was 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:

- Ersetzen *{ORIGINATION_PHONE_NUMBER_ID}* mit der ID Ihrer Telefonnummer.
- Ersetzen *{BUCKET}* durch den Namen des Amazon S3 S3-Buckets.
- Ersetzen *{MEDIA_FILE}* durch den Namen der Mediendatei.

Sie können auch mit einer Presign-URL hochladen, indem Sie `--source-s3-presigned-url` anstelle von `--source-s3-file` verwenden. Sie müssen das Header-Feld hinzufügen`Content-Type`. 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
```

Gehen Sie im vorhergehenden Befehl wie folgt vor:

- Ersetzen *{PHONE_NUMBER}* durch die Telefonnummer Ihrer Kunden.
- Ersetzen *{ORIGINATION_PHONE_NUMBER_ID}* mit der ID Ihrer Telefonnummer.
- Ersetzen *{MEDIA_ID}* durch die Medien-ID, die Sie aus dem vorherigen Schritt erhalten.

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:

- Ersetzen *{ORIGINATION_PHONE_NUMBER_ID}* mit der ID Ihrer Telefonnummer.
- Ersetzen *{MEDIA_ID}* mit der Medien-ID.

Auf eine empfangene Nachricht in AWS End User Messaging Social antworten

Bevor Sie eine Text- oder Mediennachricht empfangen können, müssen Sie die Einrichtung Ihres Ziels WABA und die Einrichtung eines Veranstaltungsziels abgeschlossen haben. Wenn Sie eine eingehende Nachricht erhalten, wird ein Ereignis im SNS Amazon-Zielthema für das Ereignis gespeichert. Sie müssen den SNS Amazon-Themen-Endpunkt abonnieren, um eine Benachrichtigung zu erhalten.

Ein Beispiel für ein Ereignis im Zusammenhang mit einer empfangenen Medienmitteilung finden Sie unterBeispiel WhatsApp JSON 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 aktiviert habenWABA, siheFügen Sie eine Nachricht und ein Ereignisziel zu AWS End User Messaging Social hinzu.

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

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:

- Ersetzen *{ORIGINATION_PHONE_NUMBER_ID}* mit der ID Ihrer Telefonnummer.

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

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

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

- Ersetzen *{MEDIA_ID}* mit dem Wert des ID-Felds aus dem empfangenen Ereignis. Ein Beispiel für ein eingehendes Medienereignis finden Sie unterBeispiel WhatsApp JSON für den Empfang einer Mediennachricht.
- Ersetzen *{ORIGINATION_PHONE_NUMBER_ID}* mit der 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:

- Ersetzen *{BUCKET}* durch den Namen des Amazon S3 S3-Buckets.
- Ersetzen *{MEDIA_ID}* durch die MEDIA _ID, die Sie aus dem vorherigen Schritt erhalten.

Beispiel für die Beantwortung einer Nachricht mit einem Lesen 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

Sie müssen ein SNS Amazon-Thema für das Eventziel eingerichtet und einen der Themen-Endpunkte abonniert haben, um eine Benachrichtigung zu erhalten, dass Diego eine Nachricht gesendet hat.

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 Ihre geschäftlich initiierten Konversationen angerechnet.

```
{
  "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"
    }
  ]
}
  {
  "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 anzuzeigen, dass Sie die Nachricht erhalten haben, setzen Sie den Status auf`read`. Diego sieht zwei blaue Häkchen neben der Nachricht auf seinem Gerät.

```
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:

   - Ersetzen *{ORIGINATION_PHONE_NUMBER_ID}* mit der Telefonnummer-ID, an die Diego seine Nachricht gesendet hat`phone-number-id-976c72a700aac43eaf573ae050example`.
   - Ersetzen *{MESSAGE_ID}* mit der eindeutigen Kennung der Nachricht. Dies ist derselbe Wert wie die ID in der empfangenen Nachricht`wamid.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:

   - Ersetzen *{PHONE_NUMBER}* mit Diegos Telefonnummer`14255550150`.
   - Ersetzen *{MESSAGE_ID}* mit der eindeutigen Kennung der Nachricht. Dies ist derselbe Wert wie die ID in der empfangenen Nachricht`wamid.HBgLMTQyNTY5ODgzMDIVAgASGCBDNzBDRjM5MDU2ODEwMDkwREY4ODBDRDE0Rj`

- Ersetzen *{ORIGINATION_PHONE_NUMBER_ID}* mit der Telefonnummer-ID, 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 API Cloud-Referenz.

WhatsApp -Fakturierungs- und Nutzungsberichte für AWS End User Messaging Social verstehen

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 Preise für AWS End User Messaging.

Feld	Optionen	Beschreibung
`Region code`	• USE1— Region USA Ost (Nord-Virginia) • USE2— Region USA Ost (Ohio) • USW1— Region USA West (Oregon) • APS1— Region Asien-Pazifik (Mumbai) • APSE1— Region Asien-Pazifik (Singapur) • EUW1— Region Europa (Irland)	Das AWS-Region -Präfix, das angibt, von wo die WhatsApp Nachricht gesendet oder empfangen wurde.

Feld	Optionen	Beschreibung
	• EUW2— Region Europa (London)	
MessagingType	`WhatsApp`	Dieses Feld identifiziert den Nachrichtentyp, der gesendet wird.
ISO	Siehe unterstützte Länder	Der zweistellige ISO Ländercode, an den die Nachricht gesendet wurde.
FeeDescription	`ConversationFee` , `MessageFee`	In diesem Feld wird entweder der WhatsApp `ConversationFee` oder der AWS per angegeben. `MessageFee`

Feld	Optionen	Beschreibung
FeeType	`Authentication` , `Marketing` , `Service`, `Utility`, `Standard`	In diesem Feld wird angezeigt , welche Art von Konversat ion verwendet wurde, oder es gibt die Standardgebühr pro Nachricht an Vom Unternehmen initiiert e **`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/Ange bote und Erinnerungen an abgebrochene Einkaufsw agen. • `Utility`— Wird verwendet , um Benutzeraktionen oder Anfragen nachzuver folgen. Beispiele hierfür sind Opt-in-Bestätigung, Bestell-/Liefermanagement (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). • `Service`— Wird zur Lösung von Kundenanf ragen verwendet. Vom Benutzer initiierte **`ConversationFee`** Kategorien • `Service`— Wird zur Lösung von Kundenanf ragen verwendet. **`MessageFee`** -Kategorien • `Standard`— Gebühr pro gesendeter oder empfangen er 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
```

Beispiel 1: Senden einer Marketing-Template-Nachricht

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 ISORechnungscodes für Endbenutzer-Messaging, Social und WhatsApp Zuordnung der Gesprächsgebühren

Land des Landes

ISOLandesvorwahl mit zwei Ziffern	Ländername	WhatsApp Region für die Abrechnung der Konversation
AF	Afghanistan	Regionen in Asien-Pazifik
AXT	Asien-Pazifik	Sonstige
AL	Albanien	Rest Mittel- und Osteuropas
DZ	Algerien	Afrika
AS	Amerikanisch-Samoa	Sonstige
AD	Andorra	Sonstige
AO	Angola	Afrika
AI	Anguilla	Sonstige
AQ	Antarktis	Sonstige
AG	Antigua und Barbuda	Sonstige
AR	Argentinien	Argentinien
AM	Armenien	Rest Mittel- und Osteuropas
AW	Aruba	Sonstige
AC	Asien-Pazifik	Sonstige
AU	Australien	Regionen in Asien-Pazifik
AT	Österreich	Rest Westeuropas
AZ	Aserbaidschan	Rest Mittel- und Osteuropas

ISOLandesvorwahl mit zwei Ziffern	Ländername	WhatsApp Region für die Abrechnung der Konversation
BS	Bahamas	Sonstige
BH	Bahrain	ME: Naher Osten
BD	Bangladesch	Regionen in Asien-Pazifik
BB	Barbados	Sonstige
BY	Belarus	Rest Mittel- und Osteuropas
BE	Belgien	Rest Westeuropas
BZ	Belize	Sonstige
BJ	Benin	Afrika
BM	Bermuda	Sonstige
BT	Bhutan	Sonstige
BO	Bolivien	Rest Lateinamerikas
BQ	Bonaire	Sonstige
BA	Bosnien und Herzegowina	Sonstige
BW	Botswana	Afrika
BV	Bouvet-Insel	Sonstige
BR	Brasilien	Brasilien
IO	Britisches Territorium im Indischen Ozean	Sonstige
VG	Britische Jungferninseln	Sonstige
BN	Brunei Darussalam	Sonstige

ISOLandesvorwahl mit zwei Ziffern	Ländername	WhatsApp Region für die Abrechnung der Konversation
BG	Bulgarien	Rest Mittel- und Osteuropas
BF	BurkinaFaso	Afrika
BI	Burundi	Afrika
KH	Kambodscha	Regionen in Asien-Pazifik
CM	Kamerun	Afrika
CA	Kanada	Nordamerika
CV	Kap Verde	Sonstige
KY	Kaimaninseln	Sonstige
CF	Zentralafrikanische Republik	Sonstige
TD	Tschad	Afrika
CL	Chile	Chile
CN	China	Regionen in Asien-Pazifik
CX	Weihnachtsinsel	Sonstige
CC	Cocos (Keeling) Inseln	Sonstige
CO	Kolumbien	Kolumbien
KM	Komoren	Sonstige
CG	Kongo	Sonstige
CD	Kongo	Afrika
CK	Cookinseln	Sonstige
CR	Costa Rica	Rest Lateinamerikas

ISOLandesvorwahl mit zwei Ziffern	Ländername	WhatsApp Region für die Abrechnung der Konversation
CI	Elfenbeinküste	Afrika
HR	Kroatien	Rest Mittel- und Osteuropas
CW	Curaçao	Sonstige
CY	Zypern	Sonstige
CZ	Tschechische Republik	Rest Mittel- und Osteuropas
DK	Dänemark	Rest Westeuropas
DJ	Dschibuti	Sonstige
DM	Dominica	Sonstige
DO	Dominikanische Republik	Rest Lateinamerikas
EC	Ecuador	Rest Lateinamerikas
EG	Ägypten	Ägypten
SV	El Salvador	Rest Lateinamerikas
GQ	Äquatorialguinea	Sonstige
ER	Eritrea	Afrika
EE	Estland	Sonstige
ET	Äthiopien	Afrika
FK	Falklandinseln	Sonstige
FO	Färöer-Inseln	Sonstige
FJ	Fidschi	Sonstige
FI	Finnland	Rest Westeuropas

ISOLandesvorwahl mit zwei Ziffern	Ländername	WhatsApp Region für die Abrechnung der Konversation
FR	Frankreich	Frankreich
GF	Französisch-Guayana	Sonstige
PF	Französisch-Polynesien	Sonstige
TF	Französische Südgebiete	Sonstige
GA	Gabun	Afrika
GM	Gambia	Afrika
GE	Georgien	Rest Mittel- und Osteuropas
DE	Deutschland	Deutschland
GH	Ghana	Afrika
GI	Gibraltar	Sonstige
GR	Griechenland	Rest Mittel- und Osteuropas
GL	Grönland	Sonstige
GD	Grenada	Sonstige
GP	Guadeloupe	Sonstige
GU	Guam	Sonstige
GT	Guatemala	Rest Lateinamerikas
GG	Guernsey	Sonstige
GN	Guinea	Sonstige
GW	Guinea-Bissau	Afrika
GY	Guyana	Sonstige

ISOLandesvorwahl mit zwei Ziffern	Ländername	WhatsApp Region für die Abrechnung der Konversation
HT	Haiti	Rest Lateinamerikas
HM	Heard und McDonald Inseln	Sonstige
HN	Honduras	Rest Lateinamerikas
HK	Hong Kong	Regionen in Asien-Pazifik
HU	Ungarn	Rest Mittel- und Osteuropas
IS	Island	Sonstige
IN	Indien	Indien
IN	Asien-Pazifik	Asien-Pazifik
ID	Indonesien	Indonesien
ID	Indonesia International	Indonesia International
IQ	Irak	ME: Naher Osten
IE	Irland	Rest Westeuropas
IM	Isle of Man	Sonstige
IL	Israel	Israel
IT	Italien	Italien
JM	Jamaika	Rest Lateinamerikas
JP	Japan	Rest in Asien-Pazifik
JE	Jersey	Sonstige
JO	Jordanien	ME: Naher Osten
KZ	Kasachstan	Sonstige

ISOLandesvorwahl mit zwei Ziffern	Ländername	WhatsApp Region für die Abrechnung der Konversation
KE	Kenia	Afrika
KI	Kiribati	Sonstige
XK	Kosovo	Sonstige
KW	Kuwait	ME: Naher Osten
KG	Kirgisistan	Sonstige
LA	Laotisch PDR	Rest in Asien-Pazifik
LV	Lettland	Rest Mittel- und Osteuropas
LB	Libanon	ME: Naher Osten
LS	Lesotho	Afrika
LR	Liberia	Afrika
LY	Libyen	Afrika
LI	Liechtenstein	Sonstige
LT	Litauen	Rest Mittel- und Osteuropas
LU	Luxemburg	Sonstige
MO	Macau	Sonstige
MK	Mazedonien	Restliches Mittel- und Osteuropa
MG	Madagaskar	Afrika
MW	Malawi	Afrika
MY	Malaysia	Malaysia

ISOLandesvorwahl mit zwei Ziffern	Ländername	WhatsApp Region für die Abrechnung der Konversation
MV	Malediven	Sonstige
ML	Mali	Afrika
MT	Malta	Sonstige
MH	Marshallinseln	Sonstige
MQ	Martinique	Sonstige
MR	Mauretanien	Afrika
MU	Mauritius	Sonstige
YT	Mayotte	Sonstige
MX	Mexiko	Mexiko
FM	Mikronesien	Sonstige
MD	Moldau	Rest Mittel- und Osteuropas
MC	Monaco	Sonstige
MN	Mongolei	Rest in Asien-Pazifik
ME	Montenegro	Sonstige
MS	Montserrat	Sonstige
MA	Marokko	Afrika
MZ	Mosambik	Afrika
MM	Myanmar	Sonstige
N/A	Namibia	Afrika
NR	Nauru	Sonstige

ISOLandesvorwahl mit zwei Ziffern	Ländername	WhatsApp Region für die Abrechnung der Konversation
NP	Nepal	Rest in Asien-Pazifik
NL	Niederlande	Niederlande
NC	Neukaledonien	Sonstige
NZ	Neuseeland	Rest in Asien-Pazifik
NI	Nicaragua	Rest Lateinamerikas
NE	Niger	Afrika
NG	Nigeria	Nigeria
NU	Niue	Sonstige
NF	Norfolkinsel	Sonstige
MP	Nördliche Marianen	Sonstige
NO	Norwegen	Rest Westeuropas
OM	Oman	ME: Naher Osten
PK	Pakistan	Pakistan
PW	Palau	Sonstige
PS	Palästinensisches Hoheitsgebiet	Sonstige
PA	Panama	Rest Lateinamerikas
PG	Papua-Neuguinea	Rest in Asien-Pazifik
PY	Paraguay	Rest Lateinamerikas
PE	Peru	Peru

ISOLandesvorwahl mit zwei Ziffern	Ländername	WhatsApp Region für die Abrechnung der Konversation
PH	Philippinen	Rest in Asien-Pazifik
PN	Falklandinseln	Sonstige
PL	Polen	Restliches Mittel- und Osteuropa
PT	Portugal	Rest Westeuropas
PR	Puerto Rico	Rest Lateinamerikas
QA	Katar	ME: Naher Osten
RE	Wiedersehen	Sonstige
RO	Rumänien	Rest Mittel- und Osteuropas
RU	Russische Föderation	Russland
RW	Ruanda	Afrika
SH	Heiliger Martin	Sonstige
KN	St. Kitts und Nevis	Sonstige
LC	St. Lucia	Sonstige
PM	St. Pierre und Miquelon	Sonstige
VC	St. Vincent und die Grenadine n	Sonstige
BL	St. Barthélemy	Sonstige
MF	Heiliger Martin	Sonstige
WS	Samoa	Sonstige
SM	San Marino	Sonstige

ISOLandesvorwahl mit zwei Ziffern	Ländername	WhatsApp Region für die Abrechnung der Konversation
ST	São Tomé und Príncipe	Sonstige
SA	Saudi-Arabien	Saudi-Arabien
SN	Senegal	Afrika
RS	Serbien	Rest Mittel- und Osteuropas
SC	Seychellen	Sonstige
SL	Sierra Leone	Afrika
SG	Singapur	Rest in Asien-Pazifik
SX	St. Maarten	Sonstige
SK	Slowakei	Rest Mittel- und Osteuropas
SI	Slowenien	Restliches Mittel- und Osteuropa
SB	Salomoninseln	Sonstige
SO	Somalia	Afrika
ZA	Südafrika	Südafrika
GS	Südgeorgien und die Südlichen Sandwichinseln	Sonstige
KR	Südkorea	Sonstige
SS	Südsudan	Afrika
ES	Spanien	Spanien
LK	Sri Lanka	Rest in Asien-Pazifik
SR	Surinam	Sonstige

ISOLandesvorwahl mit zwei Ziffern	Ländername	WhatsApp Region für die Abrechnung der Konversation
SJ	Inseln Spitzbergen und Jan Mayen	Sonstige
SZ	Swasiland	Afrika
SE	Schweden	Rest Westeuropas
CH	Schweiz	Rest Westeuropas
TW	Taiwan	Rest in Asien-Pazifik
TJ	Tadschikistan	Rest in Asien-Pazifik
TZ	Tansania	Afrika
TH	Thailand	Rest in Asien-Pazifik
TL	Timor-Leste	Sonstige
TG	Togo	Afrika
TK	Tokelau	Sonstige
TO	Tonga	Sonstige
TT	Trinidad und Tobago	Sonstige
TA	Trist und ein Cunha	Sonstige
TN	Tunesien	Afrika
TR	Türkei	Türkei
TM	Turkmenistan	Rest in Asien-Pazifik
TC	Turks- und Caicosinseln	Sonstige
TV	Tuvalu	Sonstige

ISOLandesvorwahl mit zwei Ziffern	Ländername	WhatsApp Region für die Abrechnung der Konversation
UG	Uganda	Afrika
UA	Ukraine	Rest Mittel- und Osteuropas
AE	Vereinigte Arabische Emirate	Vereinigte Arabische Emirate
GB	Großbritannien und Nordirland	Großbritannien und Nordirland
US	Vereinigte Staaten	Nordamerika
UY	Uruguay	Rest Lateinamerikas
UM	Kleinere abgelegene Inseln in USA	Sonstige
UZ	Usbekistan	Rest in Asien-Pazifik
VU	Vanuatu	Sonstige
VA	Asien-Pazifik	Sonstige
VE	Venezuela	Rest Lateinamerikas
VN	Vietnam	Rest in Asien-Pazifik
VI	Asien-Pazifik	Sonstige
WF	Inseln Wallis und Futuna	Sonstige
EH	Westsahara	Sonstige
YE	Jemen	ME: Naher Osten
ZM	Sambia	Afrika
ZW	Simbabwe	Sonstige

Überwachung von Social Messaging für AWS Endbenutzer

Die Überwachung ist ein wichtiger Teil der Aufrechterhaltung von Zuverlässigkeit, Verfügbarkeit und Leistung von AWS End User Messaging Social und Ihren anderen AWS -Lösungen. AWSstellt die folgenden Überwachungstools zur Verfügung, um AWS End User Messaging Social zu überwachen, Sie zu informieren, wenn etwas nicht funktioniert, und gegebenenfalls automatische Maßnahmen zu ergreifen:

- Amazon CloudWatch überwacht Ihre AWS -Ressourcen und die in ausgeführten Anwendungen 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. Beispielsweise können Sie mit die CPU Nutzung oder andere Metriken Ihrer EC2 Amazon-Instances CloudWatch erfassen und bei Bedarf automatisch neue Instances starten. Weitere Informationen finden Sie im CloudWatch Amazon-Benutzerhandbuch.
- Amazon CloudWatch Logs ermöglicht Ihnen die Überwachung, Speicherung und den Zugriff auf Ihre Protokolldateien von EC2 Amazon-Instances CloudTrail, und anderen Quellen. CloudWatch Protokolle können 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 erfolgten, und übermittelt die Protokolldateien an einen von Ihnen angegebenen Amazon-S3-Bucket. Sie können die Benutzer und Konten, die aufgerufen haben AWS, identifizieren, sowie die Quell-IP-Adresse, von der diese Aufrufe stammen, und den Zeitpunkt der Aufrufe ermitteln. Weitere Informationen finden Sie im AWS CloudTrail -Benutzerhandbuch.

Überwachung von Social Messaging für AWS Endbenutzer mit Amazon CloudWatch

Sie können die Verwendung von AWS Endbenutzer-Nachrichten in Social überwachen CloudWatch, wobei Rohdaten erfasst und in lesbare, nahezu Echtzeit-Metriken verarbeitet werden. 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.

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

Dimension	Beschreibung
MessageFeeType	Gültige Gebührentypen sind Service, Marketing, Utility und Authentifizierung
DestinationCountryCode	Der ISO zweibuchstabige Code für das Land
WhatsAppPhoneNumberArn	Der Arn der Telefonnummer

Protokollieren von Social API Media-Anrufen für AWS Endbenutzer mithilfe von AWS CloudTrail

AWS ORC ist mit integriert AWS CloudTrail, einem Service, der eine Aufzeichnung der von einem Benutzer, einer Rolle oder einem Service in Amazon EKS durchgeführten Aktionen bietet AWS-Service. CloudTrail erfasst alle API Aufrufe von AWS End User Messaging Social als Ereignisse. Zu den erfassten Aufrufen gehören Aufrufe von der AWS OpenSearch-Servicekonsole und Code-Aufrufe der AWS API OpenSearch-Serverless-API-Operationen von Amazon EMR in EKS. Mit den

von CloudTrail gesammelten Informationen können Sie die an gestellte AWS Anfrage, von der die Anfrage gestellt wurde, den Initiator der Anfrage bestimmen.

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.
- Das folgende Beispiel zeigt einen CloudTrail-Protokolleintrag in IAM das Apache.
- 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 Das Erstellen eines AWS-Konto Eventverlaufs stellt eine Aufzeichnung der CloudTrail Ereignisse in Ihrem Konto dar. Der CloudTrail Ereignisverlauf stellt eine anzeigbare, durchsuchbare und unveränderliche Aufzeichnung der Verwaltungsereignisse der letzten 90 Tage in einer bereit. AWS-Region Weitere Informationen finden Sie im AWS CloudTrail Benutzerhandbuch unter Arbeiten mit dem CloudTrail Ereignisverlauf. Für die Anzeige des Eventverlaufs CloudTrail fallen keine CloudTrails an.

Um Aktivitäten und Ereignisse in Ihrem fortlaufend AWS-Konto aufzuzeichnen, erstellen Sie einen Trail für eine einzelne Aufzeichnung CloudTrailder Ereignisse in Ihrem Konto.

CloudTrail Pfade

Ein Trail ermöglicht es CloudTrail CloudTrail, Protokolldateien in einem Amazon-S3-Bucket bereitzustellen. Trails, die mit der Konsole erstellt wurden, AWS Management Console sind multiregional. Sie können nur einen einzelnen Regions-Trail erstellen, indem Sie die verwenden. AWS CLI Das Erstellen eines Trails mit mehreren Regionen wird als bewährte Methode empfohlen, da Sie Aktivitäten in allen Regionen AWS-Regionen in Ihrem Konto erfassen. Sie können nur einen einzelnen Regions-Trail erstellen, indem Sie die verwenden. AWS-Region Weitere Informationen zu Trails finden Sie unter Einen Trail für Sie erstellen AWS-Konto und Einen Trail für eine Organisation erstellen im AWS CloudTrail Benutzerhandbuch.

Sie können einen Trail erstellen, CloudTrail indem Sie einen Trail Amazon S3. Weitere Informationen zur CloudTrail Preisgestaltung finden Sie unter AWS CloudTrail Preise. Informationen zu Amazon-S3-Preisen finden Sie unter Amazon S3-Preise.

CloudTrail CloudTrail-Ereignisdatenspeicher

CloudTrail Mit Lake können Sie SQL feinKÖRnige SQL-basierte Abfragen zu Ihren Ereignissen ausführen. CloudTrail CloudTrail Lake konvertiert vorhandene Ereignisse im zeilenbasierten JSON-Format in das Apache JSON ORC ORC -Format. ORCORC ist ein spaltenförmiges Speicherformat, das für den schnellen Abruf von komprimierten 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 im AWS CloudTrail Benutzerhandbuch unter Arbeiten mit AWS CloudTrail Lake.

CloudTrail Für -Lake-Ereignisdatenspeicher und -abfragen fallen Gebühren 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. Standardmäßig werden Datenereignisse CloudTrail nicht von den Trails protokolliert. 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 protokollieren AWS CLI, indem Sie die CloudTrail Konsole oder CloudTrail API Operationen verwenden. Weitere Informationen zum Protokollieren von Datenereignissen finden Sie unter Protokollieren von Datenereignissen mit der AWS Management Console und Protokollieren von Datenereignissen mit dem AWS Command Line Interface im AWS CloudTrail Benutzerhandbuch.

In der folgenden Tabelle sind die Ressourcentypen von 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 APIsProtokollierte 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 `resources.ARN` Felder`eventName`, und filtern`readOnly`, sodass nur die Ereignisse protokolliert werden, die für Sie wichtig sind. Weitere Informationen zu diesen Feldern finden Sie unter. AdvancedFieldSelectorin der AWS CloudTrail APIReferenz.

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

Verwaltungsereignisse liefern Einblicke in die Verwaltungsoperationen, die für Ressourcen im -Konto ausgeführt wurden AWS-Konto. Sie werden auch als Vorgänge auf Steuerebene bezeichnet. Standardmäßig werden Datenereignisse CloudTrail protokolliert.

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 APIReferenz zu AWS End User Messaging Social.

AWS Beispiele für Ereignisse in Form von End User Messaging Social

Ein Ereignis stellt eine einzelne Anfrage aus einer beliebigen Quelle dar und enthält unter anderem Informationen über die angeforderte API Aktion. CloudTrail CloudTrail-Protokolldateien sind kein geordnetes Stack-Trace der öffentlichen API API-Aufrufe und erscheinen daher in keiner bestimmten Reihenfolge.

Das folgende Beispiel zeigt einen CloudTrail -Protokolleintrag, der die -Operation 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 dabei helfen können, die Kundenbindung zu verbessern und die Sperrung von Konten 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. Die folgenden Opt-in-Regionen werden unterstützt:

- 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 Empfänger über ein Onlineformular angeben können, dass sie Ihre Nachrichten erhalten möchten, verhindern Sie, dass automatisierte Scripts ohne Wissen der Benutzer Abonnements für sie abschließen. Beschränken Sie auch die Häufigkeit, mit der ein Benutzer in einer einzelnen Sitzung eine Telefonnummer angeben kann.

Respektieren Sie alle Anfragen einer Person, unabhängig davon, ob diese Person WhatsApp aktiviert oder deaktiviert ist, die Kommunikation zu blockieren, einzustellen oder auf andere Weise 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 Sie eine WhatsApp serviceverknüpfte Rolle mit IAM:

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 Scheme	• Work-from-home programme • Risiko-Investitionschancen • Pyramiden- oder mehrstufige Vermarktu ngssysteme
Illegale Substanzen	• Cannabis/CBD 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
Lead-Generierung 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 nur während der normalen Geschäftszeiten am jeweiligen Tag. Wenn Sie Nachrichten zur Mittagszeit oder mitten in der Nacht senden, ist es sehr wahrscheinlich, dass Kunden Ihre Nachrichten abbestellen, 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

Die Sicherheit in der Cloud hat bei AWS höchste Priorität. Als AWS -Kunde profitieren Sie von Rechenzentren und Netzwerkarchitekturen, die eingerichtet wurden, um die Anforderungen der anspruchsvollsten Organisationen in puncto Sicherheit zu erfüllen.

Sicherheit ist eine übergreifende Verantwortlichkeit zwischen AWS und Ihnen. Das Modell der geteilten Verantwortung beschreibt dies als Sicherheit der Cloud selbst und Sicherheit in der Cloud:

- Sicherheit der Cloud — AWS ist zuständig für den Schutz der Infrastruktur, die AWS -Services in der ausführt AWS Cloud. AWS AWS stellt Ihnen Dienste bereit, die Sie sicher verwenden können. Auditoren von Drittanbietern testen und überprüfen die Effektivität unserer Sicherheitsmaßnahmen im Rahmen der -Compliance-Programme -Compliance-Programme -Compliance-Programme - Compliance-Programme -Compliance-Programme -Compliance-Programme AWS -Compliance-Programme AWS - Informationen zu den Compliance-Programmen, die für AWS End User Messaging Social gelten, finden Sie AWS unter AWS
- Sicherheit in der Cloud — Ihr Verantwortungsumfang wird durch den AWS -Service bestimmt, den Sie verwenden, bestimmt. 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 übergreifenden Verantwortlichkeit bei der Verwendung von AWS End User Messaging Social einsetzen können. In den folgenden Themen erfahren Sie, wie Sie AWS End User Messaging Social zur Erfüllung Ihrer Sicherheits- und Compliance-Ziele konfigurieren können. Sie lernen auch, wie Sie andere AWS -Services verwenden, die Sie bei der Überwachung und beim Backup Ihrer AWS End-User-Messaging-Ressourcen unterstützen.

Themen

- Bewährte Methoden für die Gewährleistung der Sicherheit
- Verwenden von serviceverknüpften AWS Rollen für Amazon

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 die gesamte ausgeführt wird 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 Datenschutz FAQ. Informationen zum Datenschutz in Europa finden Sie im -Modell der AWS geteilten Verantwortung und den GDPR Blog-Beitrag im Blog zur AWS -Sicherheit.

Aus Datenschutzgründen empfehlen wir, AWS-Konto -Anmeldeinformationen zu schützen und einzelne Benutzer mit AWS IAM Identity Center oder AWS Identity and Access Management (IAM) einzurichten. 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-Factor Authentication (MFAMFA).
- Verwenden SieSSL/TLS, um mit AWS Ressourcen zu kommunizieren. Wir benötigen TLS TLS 1.2 und empfehlen TLS TLS 1.2.
- Richten Sie die API 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 Standardsicherheitskontrollen in 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 auf AWS über eine Befehlszeilenschnittstelle oder über eine Befehlszeilenschnittstelle FIPS 140-3 validierte kryptografische Module benötigenAPI, verwenden Sie einen Endpunkt. FIPS Weitere Informationen über verfügbare FIPS Endpunkte finden Sie unter Bundesstandard für Informationsprozesse (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 arbeiten,API, AWS CLI oder. 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 an einen externen Server bereitstellen, empfehlen wir dringend, Sie keine Anmeldeinformationen zur Validierung Ihrer Anforderung URL an den betreffenden Server 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 während der Übertragung und im Ruhezustand innerhalb der AWS Grenze verschlüsselt. Wenn Sie Daten an AWS End User Messaging Social senden, werden die Daten beim Empfang verschlüsselt und gespeichert. Wenn Sie Daten aus AWS End User Messaging Social abrufen, werden die Daten mithilfe der aktuellen 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 Service 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 Transport Layer Security (TLS) 1.2 für die Kommunikation mit Ihren Clients, Anwendungen und Meta. Um mit anderen AWS Diensten zu

kommunizieren, verwendet AWS End User Messaging Social HTTPS und TLS 1.2. Wenn Sie AWS SMS Ressourcen mithilfe der Konsole erstellen und verwalten, wird außerdem die AWS Command Line Interface gesamte Kommunikation mit HTTPS und TLS 1.2 gesichert. AWS SDK

Schlüsselverwaltung

Um Ihre Daten zu verschlüsseln, verwendet AWS End User Messaging Social interne AWS KMS -Schlüssel, die der Service besitzt und in Ihrem Namen verwaltet. Diese Schlüssel werden regelmäßig rotiert. Sie können keine eigenen AWS KMS oder anderen Schlüssel bereitstellen und verwenden, um Daten zu verschlüsseln, die Sie in AWS End User Messaging Social speichern.

Datenschutz für den Datenverkehr zwischen Netzwerken

Richtlinie für den Datenverkehr zwischen Netzwerken bezieht sich auf die Sicherung von Verbindungen und Datenverkehr zwischen AWS End User Messaging Social und Ihren Clients und Anwendungen vor Ort sowie zwischen AWS End User Messaging Social und anderen AWS Ressourcen in denselben. AWS-Region Die folgenden Features und Praktiken können Ihnen dabei helfen, den Schutz des Netzwerkverkehrs für AWS End User Messaging Social sicherzustellen.

Datenverkehr zwischen AWS SMS und Clients und Anwendungen vor Ort

Um eine private Verbindung zwischen AWS End User Messaging Social und Clients und Anwendungen in Ihrem 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 Versionen zu sichernAPIs, empfehlen wir Ihnen, die Anforderungen von AWS End User Messaging Social Social für API Anrufe einzuhalten. AWS End User Messaging Social verlangt von Kunden die Verwendung von Transport Layer Security (TLS) 1.2 oder höher. Clients müssen außerdem Cipher Suites mit Perfect Forward Secrecy (PFS) wie Ephemeral Diffie-Hellman () oder Elliptic Curve Diffie-Hellman Ephemeral (DHE) unterstützen. ECDHE Die meisten modernen Systeme wie Java 7 und höher unterstützen diese Modi.

Außerdem müssen Anforderungen mit einer Zugriffsschlüssel-ID und einem geheimen Zugriffsschlüssel signiert sein, der mit einem AWS Identity and Access Management (IAM) -Prinzipal

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

Identity and Access AWS Management für Client

AWS Identity and Access Management (IAM) hilft einem Administrator AWS-Service , den Zugriff auf AWS Ressourcen sicher zu kontrollieren. IAMAdministratoren steuern, wer authentifiziert (angemeldet) und autorisiert (Berechtigungen besitzt) ist, -Ressourcen von AWS End User Messaging Social zu nutzen. IAMIAM ist ein AWS-Service , den Sie ohne zusätzliche Kosten verwenden können.

Themen

Zielgruppe

Wie Sie AWS Identity and Access Management (IAM) verwenden, unterscheidet sich je nach Ihrer Arbeit in AWS End User Messaging Social.

Service-Benutzer — Wenn Sie den AWS End User Messaging Social -Service zur Ausführung von Aufgaben verwenden, stellt Ihnen Ihr Administrator die Anmeldeinformationen und Berechtigungen bereit, die Sie benötigen. Wenn Sie für Ihre Arbeit weitere Funktionen in AWS End User Messaging Social ausführen, benötigen Sie möglicherweise zusätzliche Berechtigungen. Wenn Sie die Fuktionsweise der Zugriffskontrolle nachvollziehen, wissen Sie bereits, welche Berechtigungen Sie von Ihrem Administrator anzufordern müssen. Unter finden Sie nützliche Informationen für den Fall, dass Sie keinen Zugriff auf eine Feature in AWS End User Messaging Social habenProblembehebung bei AWS Endbenutzer-Nachrichten Soziale Identität und Zugriff.

Service administrator (Service-Administrator) — Wenn Sie in Ihrem Unternehmen für die Ressourcen von AWS End User Messaging Social verantwortlich sind, haben Sie wahrscheinlich vollständigen

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 Service-Benutzer zugreifen sollen. Sie müssen anschließend Anträge an Ihren IAM -Administrator stellen, um die Berechtigungen Ihrer Dienstnutzer zu ändern. Lesen Sie die Informationen auf dieser Seite, um die Grundkonzepte von zu verstehenIAM. Weitere Informationen dazu, wie Ihr Unternehmen AWS End User Messaging Social verwenden IAM kann, finden Sie unterSo funktioniert AWS End User Messaging Social mit IAM.

IAMadministrator — Wenn Sie als IAM Administrator fungieren, sollten Sie Einzelheiten dazu kennen, wie Sie Richtlinien zur Verwaltung des Zugriffs auf AWS End User Messaging Social verfassen können. Beispiele für identitätsbasierte Richtlinien für AWS Endnutzer-Messaging in sozialen Netzwerken, die Sie in verwenden könnenIAM, finden Sie unter. Beispiele für identitätsbasierte Richtlinien AWS für API

Authentifizierung mit Identitäten

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

Sie können sich bei AWS als Verbundidentität mit Anmeldeinformationen anmelden, die über eine Identitätsquelle bereitgestellt werden. AWS IAM Identity Center (IAMIdentity Center), die Single-Sign-on-Authentifizierung Ihres Unternehmens und Anmeldeinformationen für Google oder Facebook sind Beispiele für Verbundidentitäten. Wenn Sie sich als Verbundidentität anmelden, hat der Administrator vorher mithilfe von IAM -Rollen einen Identitätsverbund eingerichtet. Wenn Sie auf AWS mithilfe des Verbunds zugreifen, übernehmen Sie indirekt eine Rolle.

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

Bei AWS programmgesteuerten Zugriff auf AWS bietet ein Software Development Kit (SDK) und eine Befehlszeilenschnittstelle (CLI) zum kryptographischen Signieren Ihrer Anforderungen mit Ihren Anmeldeinformationen. Wenn Sie keine AWS -Tools verwenden, müssen Sie Anforderungen selbst signieren. Weitere Informationen zur Verwendung der empfohlenen Methode zum eigenen Signieren von Anforderungen finden Sie unter Signieren von AWS API Anforderungen im IAM-Benutzerhandbuch.

Unabhängig von der verwendeten Authentifizierungsmethode müssen Sie möglicherweise zusätzliche Sicherheitsinformationen angeben. AWS empfiehlt beispielsweise die Verwendung von Multi-Factor Authentication (MFA), um die Sicherheit Ihres Kontos zu verbessern. Weitere Informationen finden Sie unter Multi-Faktor-Authentifizierung im AWS IAM Identity Center Benutzerhandbuch und Verwenden der Multi-Faktor-Authentifizierung (MFA) AWS im IAM Benutzerhandbuch.

AWS-Konto -Stammbenutzer

Wenn Sie ein erstellen AWS-Konto, beginnen Sie mit einer Anmeldeidentität, die vollständigen Zugriff auf alle AWS-Services und Ressourcen des Kontos hat. Diese Identität wird als AWS-Konto -Root-Benutzer bezeichnet, auf den Sie zugreifen können, indem Sie sich mit der E-Mail-Adresse und dem Passwort anmelden, die zur Erstellung des Kontos verwendet wurden. Wir raten ausdrücklich davon ab, den Root-Benutzer für Alltagsaufgaben zu verwenden. Schützen Sie Ihre Root-Benutzer-Anmeldeinformationen und verwenden Sie diese, 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 empfiehlt es sich, menschliche Benutzer, einschließlich Benutzer, die Administratorzugriff benötigen, aufzufordern, den Verbund mit einem Identitätsanbieter zu verwenden, AWS-Services um auf mit temporären Anmeldeinformationen zuzugreifen.

Eine Verbundidentität ist ein Benutzer aus dem Benutzerverzeichnis Ihres Unternehmens, ein Web Identity Provider, AWS Directory Service, das Identity-Center-Verzeichnis oder jeder Benutzer, der mit Anmeldeinformationen, die über eine AWS-Services Identitätsquelle bereitgestellt werden, auf zugreift. Wenn Verbundidentitäten auf 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 mit einer Gruppe von Benutzern und Gruppen in Ihrer eigenen Identitätsquelle herstellen und synchronisieren, um sie in allen AWS-Konten und 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 Entität in Ihrem AWS-Konto System mit bestimmten Berechtigungen für eine einzelne Person oder eine einzelne Anwendung. 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 Sie Zugriffsschlüssel für Anwendungsfälle, die langfristige Anmeldeinformationen erfordern im IAMBenutzerhandbuch.

Eine IAMGruppe 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 einer Gruppe mit dem Namen IAMAdminsBerechtigungen zum Verwalten von IAM -Ressourcen gewähren.

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 Wann sollte ein IAM Benutzer (statt einer Rolle) erstellt werden? im IAMBenutzerhandbuch.

IAMRollen

Eine IAMRolle ist eine Identität innerhalb von Ihnen AWS-Konto , für die bestimmte Berechtigungen gelten. Sie ist einem IAM -Benutzer vergleichbar, jedoch nicht mit einer bestimmten Person verknüpft. Sie können vorübergehend eine IAM Rolle in der annehmen, AWS Management Console indem Sie Rollen wechseln. Sie können eine Rolle übernehmen, indem Sie eine AWS CLI AWS API OR-Operation aufrufen oder eine benutzerdefinierte Operation verwendenURL. Weitere Informationen zu Methoden für die Verwendung von Rollen finden Sie unter Methoden zur Übernahme einer Rolle im IAMBenutzerhandbuch.

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 im IAMBenutzerhandbuch unter Erstellen einer

Rolle für einen externen Identitätsanbieter. Wenn Sie IAM Identity Center verwenden, konfigurieren Sie einen Berechtigungssatz. Um zu steuern, 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.
- Kontenübergreifender Zugriff — Sie können eine IAM -Rolle verwenden, um jemandem (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. In einigen können Sie AWS-Services jedoch eine Richtlinie direkt an eine Ressource anfügen (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 IAM im IAM -Benutzerhandbuch.
- Serviceübergreifender Zugriff — Einige AWS-Services verwenden Features in anderen AWS-Services. Wenn Sie beispielsweise einen Aufruf in einem Service tätigen, führt dieser Service häufig Anwendungen in Amazon aus EC2 oder speichert Objekte in Amazon S3. 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 Rolle zum Ausführen von Aktionen in verwenden AWS, gelten Sie als Prinzipal. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service initiieren. FASverwendet die Berechtigungen des Prinzipals, der einen aufruft AWS-Service, in Kombination mit der Anforderung AWS-Service an den, Anforderungen an nachgelagerte Services zu stellen. FASAnforderungen werden nur dann gestellt, wenn ein Dienst eine Anforderung erhält, die Interaktionen mit anderen AWS-Services oder Ressourcen erfordert, um abgeschlossen werden zu können. 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 von innen erstellen, ändern und löschenIAM. Weitere Informationen finden Sie im IAMBenutzerhandbuch unter Erstellen einer Rolle zum Delegieren von Berechtigungen AWS-Service an eine.
  - Serviceverknüpfte Rolle — Eine serviceverknüpfte Rolle ist ein Typ von Servicerolle, die mit einem verknüpft ist. AWS-Service Der Service kann die Rolle übernehmen, um eine Aktion in

Ihrem Namen auszuführen. Serviceverknüpfte Rollen werden in Ihrem angezeigt AWS-Konto und gehören zum Service. Ein IAM -Administrator kann die Berechtigungen für serviceverknüpfte 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 . Das ist eine Art von Servicerolle, die mit einem -Service EC2 verknüpft ist. Erstellen Sie ein Instance-Profil, das an die EC2 Instance angefügt ist, um eine AWS -Rolle einer -Instance zuzuweisen und die Rolle für sämtliche Anwendungen der Instance bereitzustellen. Ein Instance-Profil enthält die Rolle und ermöglicht Programmen, die auf der EC2 Instance ausgeführt werden, temporäre Anmeldeinformationen zu erhalten. Weitere Informationen finden Sie im IAMBenutzerhandbuch unter Verwenden einer IAM Rolle zur Erteilung von Berechtigungen für Anwendungen, die auf EC2 Amazon-Instances ausgeführt werden.

Informationen darüber, ob Sie IAM Rollen oder IAM Benutzer verwenden sollten, finden Sie im Benutzerhandbuch unter Wann sollte eine IAM Rolle (anstelle eines IAM Benutzers) erstellt werden.

Verwalten des Zugriffs mit Richtlinien

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

Administratoren können mithilfe von AWS JSON Richtlinien festzulegen, wer zum Zugriff auf was berechtigt ist. Das bedeutet, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

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 aus dem AWS Management Console AWS CLI, dem oder dem abrufen AWS API.

Identitätsbasierte Richtlinien

Identitätsbasierte Richtlinien sind JSON Berechtigungsrichtliniendokumente, die Sie einer Identität anfügen können, wie z. B. Benutzern, IAM 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 Erstellen von IAM -Richtlinien im IAMBenutzerhandbuch.

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 anfügen können AWS-Konto. Verwaltete Richtlinien umfassen von AWS verwaltete und von Kunden verwaltete Richtlinien. Informationen dazu, wie Sie zwischen einer verwalteten Richtlinie und einer eingebundenen Richtlinie wählen, finden Sie unter Auswahl zwischen verwalteten und eingebundenen Richtlinien im IAMBenutzerhandbuch.

Ressourcenbasierte Richtlinien

Ressourcenbasierte Richtlinien sind JSON Richtliniendokumente, die Sie an eine Ressource anfügen. Beispiele für ressourcenbasierte Richtlinien sind IAM Rollenvertrauensrichtlinien und Amazon S3 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. Prinzipale können Konten, Verbundbenutzer oder umfassen. AWS-Services

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

Zugriffssteuerungslisten (ACLsACLs)

Zugriffskontrolllisten (ACLs) steuern, welche Prinzipale (Kontomitglieder, Benutzer oder Rollen) auf eine Ressource zugreifen können. ACLssind ähnlich wie ressourcenbasierte Richtlinien, verwenden jedoch nicht das JSON Richtliniendokumentformat.

Amazon S3 und AWS WAF Amazon VPC sind Beispiele für Dienste, die Unterstützung bietenACLs. Weitere Informationen ACLs finden Sie unter Zugriffskontrollliste (ACL) — Übersicht im Amazon Simple Storage Service-Entwicklerhandbuch.

Weitere Richtlinientypen

AWS unterstützt zusätzliche, weniger häufig verwendete 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 (IAMBenutzer 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 IAMBenutzerhandbuch.
- Service-Kontrollrichtlinien (JSONService-KontrollrichtlinienSCPs) — SCPs sind Richtlinien, die die maximalen Berechtigungen für eine Organisation oder Organisationseinheit (OU) angeben AWS Organizations. AWS Organizations ist ein Service für die Gruppierung und zentrale Verwaltung mehrerer AWS-Konten Ihres Unternehmens. Wenn Sie innerhalb einer Organisation alle Funktionen aktivieren, können Sie Service-Kontrollrichtlinien (SCPs) auf alle oder einzelne Ihrer Konten anwenden. Die SCP schränken Berechtigungen für Entitäten in Mitgliedskonten einschließlich des jeweiligen ein Root-Benutzer des AWS-Kontos. Weitere Informationen zu Organizations und SCPs finden Sie unter Richtlinien zur Servicesteuerung 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 im IAMBenutzerhandbuch unter Sitzungsrichtlinien.

Mehrere Richtlinientypen

Wenn mehrere auf eine Anforderung mehrere Richtlinientypen angewendet werden können, sind die entsprechenden Berechtigungen komplizierter. Informationen dazu, wie AWS die Zulässigkeit einer Anforderung ermittelt, wenn mehrere Richtlinientypen beteiligt sind, finden Sie unter Logik für die Richtlinienauswertung im IAMBenutzerhandbuch.

So funktioniert AWS End User Messaging Social mit IAM

Bevor Sie IAM den Zugriff auf AWS End User Messaging Social verwalten, sollten Sie sich darüber informieren, welche IAM Funktionen für AWS End User Messaging Social verfügbar sind.

IAMFunktionen, die Sie mit AWS End User Messaging Social verwenden können

IAMFunktion	AWS Nachrichtenübermittlung für Endbenutzer 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
Temporäre Anmeldeinformationen	Ja
Hauptberechtigungen	Ja
Servicerollen	Ja

IAMFunktion	AWS Nachrichtenübermittlung für Endbenutzer in sozialen Netzwerken
Service-verknüpfte Rollen	Ja

Einen Überblick über das Zusammenwirken von AWS End User Messaging Social und anderen AWS -Services mit den meisten IAM -Features finden Sie unter AWS -Services, die mit IAM Featureieren im IAM-Benutzerhandbuch.

Beispiele für identitätsbasierte Richtlinien für AWS SGW

Unterstützt Richtlinien auf Identitätsbasis: Ja

Identitätsbasierte Richtlinien sind JSON Berechtigungsrichtliniendokumente, die Sie einer Identität anfügen können, wie z. B. Benutzern, IAM 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 Erstellen von IAM -Richtlinien im IAMBenutzerhandbuch.

Mit IAM identitätsbasierten 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 können, finden Sie in der Referenz IAM JSON für Richtlinienelemente im IAMBenutzerhandbuch.

Beispiele für identitätsbasierte Richtlinien AWS für API

Beispiele für identitätsbasierte Richtlinien für AWS Endbenutzer-Nachrichten in sozialen Netzwerken finden Sie unter. Beispiele für identitätsbasierte Richtlinien AWS für API

Ressourcenbasierte Richtlinien AWS in Amazon

Unterstützt ressourcenbasierte Richtlinien: Nein

Ressourcenbasierte Richtlinien sind JSON Richtliniendokumente, die Sie an eine Ressource anfügen. Beispiele für ressourcenbasierte Richtlinien sind IAM Rollenvertrauensrichtlinien und Amazon S3 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. Prinzipale können Konten, Verbundbenutzer oder umfassen. 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 in unterschiedlichen befinden 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 IAMim IAMBenutzerhandbuch unter Kontoübergreifender Ressourcenzugriff.

Richtlinienmaßnahmen für AWS End User Messaging Social

Unterstützt Richtlinienaktionen: Ja

Administratoren können mithilfe von AWS JSON Richtlinien festzulegen, wer zum Zugriff auf was berechtigt ist. Das bedeutet, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Das `Action` Element einer JSON Richtlinie beschreibt die Aktionen, mit denen Sie den Zugriff in einer Richtlinie zulassen oder verweigern können. Richtlinienaktionen haben normalerweise denselben Namen wie die zugehörige AWS API Operation. Es gibt einige Ausnahmen, z. B. Aktionen, die nur mit Genehmigung durchgeführt werden können und für die es keinen passenden Vorgang gibt. API 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.

Richtlinienaktionen in AWS End User Messaging Social verwenden das folgende Präfix vor der Aktion:

```
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 für AWS Endbenutzer-Nachrichten in sozialen Netzwerken finden Sie unter. Beispiele für identitätsbasierte Richtlinien AWS für API

Richtlinienressourcen für AWS End User Messaging Social

Unterstützt Richtlinienressourcen: Ja

Administratoren können mithilfe von AWS JSON Richtlinien festzulegen, wer zum Zugriff auf was berechtigt ist. Das bedeutet, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Das `Resource` JSON Richtlinienelement gibt die Objekte an, auf 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 zu den Aktionen, mit denen Sie die ARN

einzelnen Ressourcen angeben können, finden Sie unter Von AWS End User Messaging Social definierte Aktionen.

Beispiele für identitätsbasierte Richtlinien für AWS Endbenutzer-Nachrichten in sozialen Netzwerken finden Sie unter. Beispiele für identitätsbasierte Richtlinien AWS für API

AWS Richtlinien-Bedingungsschlüssel für API

Unterstützt servicespezifische Richtlinienbedingungsschlüssel: Ja

Administratoren können mithilfe von AWS JSON Richtlinien festzulegen, wer zum Zugriff auf was berechtigt ist. 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 mittels 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 im IAMBenutzerhandbuch unter IAMRichtlinienelemente: Variablen und Tags.

AWS unterstützt globale Bedingungsschlüssel und serviceverknüpfte Bedingungsschlüssel.
Eine Liste aller AWS globalen -Bedingungsschlüssel finden Sie unter AWS Globale -Bedingungskontextschlüssel im IAMBenutzerhandbuch.

Eine Liste der Bedingungsschlüssel für AWS End User Messaging Social finden Sie unter Bedingungsschlüssel für AWS End User Messaging Social in der Serviceautorisierungsreferenz. 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 für AWS Endbenutzer-Nachrichten in sozialen Netzwerken finden Sie unter. Beispiele für identitätsbasierte Richtlinien AWS für API

ACLsin AWS End User Messaging Social

UnterstütztACLs: Nein

Zugriffskontrolllisten (ACLs) steuern, welche Prinzipale (Kontomitglieder, Benutzer oder Rollen) auf eine Ressource zugreifen können. ACLssind ähnlich wie ressourcenbasierte Richtlinien, verwenden jedoch nicht das JSON Richtliniendokumentformat.

ABACmit AWS End User Messaging Social

Unterstützt ABAC (Tags in Richtlinien): Teilweise

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

ABACist 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 finden Sie ABAC unter Was ist? ABAC im IAMBenutzerhandbuch. Ein Tutorial mit Schritten zur Einrichtung finden Sie im ABAC Benutzerhandbuch unter Verwenden der attributebasierten Zugriffskontrolle (ABAC). IAM

Verwenden temporärer AWS Anmeldeinformationen mit SGW

Unterstützt temporäre Anmeldeinformationen: Ja

Einige funktionieren AWS-Services nicht, wenn Sie sich mit temporären Anmeldeinformationen anmelden. Weitere Informationen, einschließlich Informationen darüber, AWS-Services wie Sie mit temporären Anmeldeinformationen arbeiten können AWS-Services , finden Sie IAM im IAMBenutzerhandbuch unter Diese Informationen.

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

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

Serviceübergreifende AWS Prinzipal-Berechtigungen für Amazon

Unterstützt Forward Access Sessions (FASFAS)

Wenn Sie einen IAM Benutzer oder eine Rolle zum Ausführen von Aktionen in verwenden AWS, gelten Sie als Prinzipal. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service initiieren. FASverwendet die Berechtigungen des Prinzipals, der einen aufruft AWS-Service, in Kombination mit der Anforderung AWS-Service an den, Anforderungen an nachgelagerte Services zu stellen. FASAnforderungen werden nur dann gestellt, wenn ein Dienst eine Anforderung erhält, die Interaktionen mit anderen AWS-Services oder Ressourcen erfordert, um abgeschlossen werden zu können. 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 IAMRolle, die ein Service übernimmt, um Aktionen in Ihrem Konto für Sie auszuführen. Ein IAM -Administrator kann eine Servicerolle von innen erstellen, ändern und

löschenIAM. Weitere Informationen finden Sie im IAMBenutzerhandbuch unter Erstellen einer Rolle zum Delegieren von Berechtigungen AWS-Service an eine.

> **Warning**
>
> Das Ändern der Berechtigungen für eine Servicerolle könnte die Funktionalität von AWS End User Messaging Social beeinträchtigen. Bearbeiten Sie Servicerollen nur, wenn AWS End User Messaging Social dazu Anleitungen gibt.

Dienstbezogene Rollen für AWS End User Messaging Social

Unterstützt dienstbezogene Rollen: Ja

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

Details zum Erstellen oder Verwalten von serviceverknüpften Rollen finden Sie unter AWS - Services, die mit IAM arbeiten. 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 AWS für API

Benutzer und Rollen haben standardmäßig nicht die Berechtigung, soziale AWS End User Messaging -Ressourcen zu erstellen oder zu ändern. Sie können auch keine Aufgaben mithilfe von AWS Management Console, AWS Command Line Interface (AWS CLI) oder ausführen AWS API. 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 zum Erstellen einer IAM identitätsbasierten Richtlinie anhand dieser JSON Beispieldokumente finden Sie unter IAMRichtlinien erstellen im IAMBenutzerhandbuch.

Einzelheiten zu den von AWS End User Messaging Social definierten Aktionen und Ressourcentypen, einschließlich des Formats der ARNs für die einzelnen Ressourcentypen, finden

Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für AWS End User Messaging Social in der Service-Autorisierungs-Referenz.

Themen

Bewährte Methoden für Richtlinien

Identitätsbasierte Richtlinien legen fest, ob jemand AWS End User Messaging-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:

- Erste Schritte mit AWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen — Um Ihren Benutzern und Workloads Berechtigungen zu gewähren, verwenden Sie die AWS -verwaltete Richtlinien die Berechtigungen für viele allgemeine Anwendungsfälle 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 spezifisch auf Ihre Anwendungsfälle zugeschnitten sind. Weitere Informationen finden Sie AWS im IAMBenutzerhandbuch unter AWS Verwaltete Richtlinien oder Verwaltete Richtlinien für Jobfunktionen.
- Anwendung von Berechtigungen mit den geringsten Rechten — Wenn Sie Berechtigungen mit IAM Richtlinien festlegen, gewähren Sie nur die Berechtigungen, die zum Ausführen 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 IAM zum Anwenden von Berechtigungen finden Sie IAMim Benutzerhandbuch unter Richtlinien und Berechtigungen. IAM
- 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 gesendet werden müssenSSL. Sie können auch Bedingungen verwenden, um Zugriff auf Service-Aktionen zu gewähren, wenn diese durch ein bestimmtes AWS-Service, wie beispielsweise, verwendet werden AWS CloudFormation. Weitere Informationen finden Sie im IAMBenutzerhandbuch unter IAMJSONRichtlinienelemente: Bedingung.

- 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 IAM bewährten Methoden entsprechen. IAMAccess Analyzer stellt mehr als 100 Richtlinienprüfungen und umsetzbare Empfehlungen zur Verfügung, damit Sie sichere und funktionale Richtlinien erstellen können. Weitere Informationen finden Sie unter IAMAccess Analyzer-Richtlinienvalidierung im IAMBenutzerhandbuch.
- Bedarf einer Multi-Faktor-Authentifizierung (MFA) — Wenn Sie ein Szenario haben, das IAM Benutzer oder Root-Benutzer in Ihrem erfordert AWS-Konto, aktivieren Sie die Option MFA für zusätzliche Sicherheit. Um festzulegenMFA, wann API Vorgänge aufgerufen werden, fügen Sie Ihren Richtlinien MFA Bedingungen hinzu. Weitere Informationen finden Sie unter Konfiguration des MFA -geschützten API Zugriffs im IAMBenutzerhandbuch.

Weitere Informationen zu bewährten Methoden finden Sie unter Bewährte Sicherheitsmethoden IAM im IAM Benutzerhandbuch. IAM

Verwenden der AWS End User Messaging Social-Konsole

Um auf die Konsole für AWS End User Messaging Social zuzugreifen, müssen Sie über einen Mindestsatz von Berechtigungen verfügen. Diese Berechtigungen müssen es Ihnen ermöglichen, Details über die Social-Ressourcen von AWS End User Messaging in Ihrem aufzulisten und anzuzeigen 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.

Für Benutzer, die nur Aufrufe an die AWS CLI oder -durchführen, müssen Sie keine Mindestberechtigungen in der Konsole erteilen AWS API. Stattdessen sollten Sie nur Zugriff auf die Aktionen zulassen, die den 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 im Benutzerhandbuch unter Hinzufügen von Berechtigungen für einen IAM Benutzer.

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 enthält Berechtigungen für die Ausführung dieser Aktion auf der Konsole oder für die programmgesteuerte Ausführung über das AWS CLI oder. AWS 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, von AWS verwaltete Richtlinien zu verwenden, als selbst Richtlinien zu schreiben. Es erfordert Zeit und Fachwissen, um von IAMKunden verwaltete Richtlinien zu erstellen, die Ihrem Team nur die benötigten Berechtigungen bieten. Um schnell loszulegen, können Sie unsere von 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 IAMBenutzerhandbuch unter AWS Verwaltete Richtlinien.

AWS -Services pflegen und aktualisieren der von AWS verwalteten Richtlinien. Die Berechtigungen in von AWS verwalteten Richtlinien können nicht geändert werden. 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. Services entfernen keine Berechtigungen aus einer von AWS verwalteten Richtlinie, so dass Richtlinienaktualisierungen Ihre vorhandenen Berechtigungen nicht beeinträchtigen.

Darüber hinaus AWS unterstützt verwaltete Richtlinien für Jobfunktionen, die mehrere Services umfassen. Die ReadOnlyAccess AWS verwaltete Richtlinie bietet beispielsweise schreibgeschützten Zugriff auf alle AWS -Services und -Ressourcen. Wenn ein Service ein neues Feature startet, AWS fügt schreibgeschützte Berechtigungen für neue Vorgänge und Ressourcen hinzu. Eine Liste und Beschreibungen der Richtlinien für Jobfunktionen finden Sie in AWS Verwaltete Richtlinien für Job-Funktionen im IAMBenutzerhandbuch.

AWS Aktualisierungen der AWS verwalteten Richtlinien in Form von End User Messaging Social

Anzeigen von Details zu Aktualisierungen für AWS -verwaltete Richtlinien für AWS End User Messaging Social, seit dieser Dienst mit der Verfolgung dieser Änderungen begonnen hat. Um automatische Warnungen über Änderungen an dieser Seite erhalten, abonnieren Sie den RSS Feed auf der Dokumentverlaufsseite AWS End User Messaging Social.

Änderung	Beschreibung	Datum
AWS End User Messaging Social hat damit begonnen, Änderungen zu verfolgen	AWS End User Messaging Social hat mit der Verfolgun g von Änderungen für seine AWS -verwalteten Richtlinien begonnen.	26. September

Problembehebung bei AWS Endbenutzer-Nachrichten Soziale Identität und Zugriff

Diagnostizieren und beheben Sie mithilfe der folgenden Informationen gängige Probleme, die bei der Verwendung von AWS End User Messaging Social und auftreten könnenIAM.

Themen

- Ich bin nicht berechtigt, eine Aktion AWS in Amazon durchzuführen.
- Ich bin nicht zur Ausführung von iam:PassRole autorisiert PassRole
- Ich möchte Personen außerhalb von mir Zugriff AWS-Konto auf meine Social-Ressourcen für AWS Endbenutzer Messaging erteilen

Ich bin nicht berechtigt, eine Aktion AWS in Amazon 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 `mateojackson` IAM Benutzer versucht, die Konsole zum Anzeigen von Details zu einer fiktiven *`my-example-widget`* Ressource zu verwenden, jedoch nicht über die fiktiven `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.

Wenden Sie sich an Ihren AWS -Administrator, falls Sie weitere Unterstützung benötigen. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

Ich bin nicht zur Ausführung von iam:PassRole autorisiert PassRole

Wenn Sie die Fehlermeldung erhalten, dass Sie nicht zum Durchführen der `iam:PassRole` Aktion autorisiert sind, müssen Ihre Richtlinien aktualisiert werden, um eine Rolle an AWS End User Messaging Social übergeben zu können.

Einige AWS-Services erlauben die Übergabe einer vorhandenen Rolle an diesen Service, sodass keine neue Servicerolle oder serviceverknüpfte Rolle erstellt werden muss. 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.

Wenden Sie sich an Ihren AWS -Administrator, falls Sie weitere Unterstützung benötigen. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

Ich möchte Personen außerhalb von mir Zugriff AWS-Konto auf meine Social-Ressourcen für AWS Endbenutzer Messaging erteilen

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. Im Fall von Services, die ressourcenbasierte Richtlinien oder Zugriffskontrolllisten (ACLs) verwenden, können Sie diese Richtlinien verwenden, um Personen Zugriff auf Ihre Ressourcen zu gewähren.

Weitere Informationen dazu finden Sie hier:

- Informationen dazu, ob AWS End User Messaging Social diese Funktionen unterstützt, finden Sie unterSo funktioniert AWS End User Messaging Social mit IAM.

- Informationen zum Gewähren des Zugriffs auf Ihre Ressourcen für alle AWS-Konten Ihre finden Sie unter Gewähren des Zugriffs IAM für einen Benutzer in einem anderen AWS-Konto Ihrer im IAM-Benutzerhandbuch.
- Informationen dazu, wie Sie -Drittanbieter Zugriff auf Ihre Ressourcen bereitstellen AWS-Konten, finden Sie unter Gewähren AWS-Konten des Zugriffs auf von externen IAM Benutzern im -Benutzerhandbuch.
- Informationen dazu, wie Sie über einen Identitätsverbund Zugriff gewähren, finden Sie unter Gewähren von Zugriff für extern authentifizierte Benutzer (Identitätsverbund) im IAM-Benutzerhandbuch.
- Informationen zu den Unterschieden zwischen der Verwendung von Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie unter Kontoübergreifender Ressourcenzugriff IAM im IAM -Benutzerhandbuch.

Konformitätsprüfung für AWS End User Messaging Social

Um zu erfahren, ob AWS-Service ein in den Geltungsbereich bestimmter Compliance-Programme fällt, siehe AWS-Services in Geltungsbereich nach Compliance-Programm AWS-Services und wählen Sie das Compliance-Programm aus, an dem Sie interessiert sind. Allgemeine Informationen finden Sie unter AWS Compliance-Programme AWS .

Die Auditberichte von Drittanbietern lassen sich mit herunterlade AWS Artifact. Weitere Informationen finden Sie unter Herunterladen von Berichten in Herunterladen von Berichten in Herunterladen von Berichten in AWS Artifact Herunterladen von Berichten in

Ihre Compliance-Verantwortung bei Verwendung AWS-Services von hängt von der Vertraulichkeit der Daten, den Compliance-Zielen des Unternehmens und den geltenden Gesetzen und Vorschriften ab. AWS stellt die folgenden Ressourcen bereit, um Sie bei der Compliance zu unterstützen:

- Kurzanleitungen für Sicherheit und Compliance — In diesen Bereitstellungsleitfäden werden Überlegungen zur Architektur erörtert und Schritte zum Bereitstellen von Basisumgebungen auf zur Verfügung AWS gestellt, die auf Sicherheit und Compliance ausgerichtet sind.
- Erstellung einer Architektur mit HIPAA Sicherheit und Compliance in Amazon Web Services — In diesem Whitepaper wird beschrieben, wie Unternehmen mithilfe von HIPAA -berechtigte AWS Anwendungen erstellen können.

> **Note**
>
> Nicht alle sind berechtigt AWS-Services . HIPAA Weitere Informationen finden Sie unter Referenz für HIPAA berechtigte Services.

- AWS -Compliance-Ressourcen AWS — Diese Arbeitsbücher und Leitfäden könnten für Ihre Branche und Ihren Standort relevant sein.
- AWS -Compliance-Leitfäden für Kunden — Verstehen Sie das Modell der geteilten Verantwortung aus dem Blickwinkel der Einhaltung von Vorschriften. In den Leitfäden werden die bewährten Methoden zum Schutz von zusammengefasst AWS-Services und die Leitlinien den Sicherheitskontrollen in verschiedenen Frameworks (einschließlich des National Institute of Standards and Technology (), des Payment Card Industry Security Standards Council () und der International Organization for Standardization (NIST)))))))), des Payment Card Industry Security Standards Council (PCI) () und der International Organization for Standardization (ISO))))))))))
- Auswertung von Ressourcen mit Regeln im AWS Config -Entwicklerhandbuch — Der AWS Config -Service bewertet, wie gut Ihre Ressourcenkonfigurationen mit internen Praktiken, Branchenrichtlinien und Vorschriften übereinstimmen.
- AWS Security Hub: Dieser AWS-Service bietet einen umfassenden Überblick über Ihren Sicherheitsstatus innerhalb von AWS. Security Hub verwendet Sicherheitskontrollen, um Ihre AWS -Ressourcen zu bewerten und Ihre Einhaltung von Sicherheitsstandards und bewährten Methoden zu überprüfen. Eine Liste der unterstützten Services und Kontrollen finden Sie in der Security-Hub-Steuerungsreferenz.
- Amazon GuardDuty — Dieser AWS-Service erkennt potenzielle Bedrohungen für Ihre AWS-Konten, Workloads, Container und Daten, indem er Ihre Umgebung auf verdächtige und böswillige Aktivitäten überwacht. GuardDuty kann Ihnen helfen, verschiedenen Compliance-Anforderungen nachzukommen PCIDSS, z. B. indem er die Anforderungen zur Erkennung von Eindringlingen erfüllt, die in bestimmten Compliance-Frameworks vorgeschrieben sind.
- AWS Audit Manager— Dieser AWS-Service hilft Ihnen, Ihre AWS -Nutzung kontinuierlich zu überprüfen, um den Umgang mit Risiken und die Compliance von Branchenstandards zu vereinfachen.

Resilienz bei Social Messaging für AWS Endbenutzer

Im Zentrum der AWS globalen -Infrastruktur stehen die AWS-Regionen und -Availability Zones. AWS-Regionen stellen mehrere physisch getrennte und isolierte Availability Zones bereit, die

über hoch redundante Netzwerke mit niedriger Latenz und hohen Durchsätzen 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 über AWS-Regionen und Availability Zones finden Sie unter AWS Globale - Infrastruktur.

Neben der AWS globalen -Infrastruktur stellt AWS End User Messaging Social verschiedene Funktionen bereit, um Ihren Anforderungen an Ausfallsicherheit und Datensicherung gerecht zu werden.

Sicherheit der Infrastruktur in AWS End User Messaging Social

Als verwalteter Service ist AWS End User Messaging Social durch die AWS globalen Verfahren zur Gewährleistung der Netzwerksicherheit von geschützt, die im Whitepaper Amazon Web Services: Übersicht über die Sicherheitsprozesse beschrieben werden.

Sie verwenden AWS veröffentlichte API Aufrufe, um über das Netzwerk auf AWS End User Messaging Social zuzugreifen. Clients müssen Transport Layer Security (TLSTLS) 1.0 unterstützen. Wir empfehlen TLS TLS 1.2 oder höher. Clients müssen außerdem Cipher Suites mit Perfect Forward Secrecy (PFS) wie (Ephemeral Diffie-Hellman) oder (Elliptic Curve DHE Ephemeral Ephemeral Diffie-Hellman) unterstützen. ECDHE Die meisten modernen Systeme 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. In AWS kann der serviceübergreifende Identitätswechsel zu Confused-Deputy-Problem 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 Verwendung der Kontextschlüssel `aws:SourceArn`und die `aws:SourceAccount`globalen Bedingungskontext-Schlüssel in Ressourcenrichtlinien zu verwenden, um die Berechtigungen einzuschränken, die Social Messaging einem anderen Service für die Ressource erteilt. 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 `aws:SourceArn` globalen Bedingungskontextschlüssels mit ARN der gesamten Ressource. Wenn Sie die Ressource nicht vollständig ARN kennen oder wenn Sie mehrere Ressourcen angeben, verwenden Sie den `aws:SourceArn` globalen Kontextbedingungsschlüssel mit Platzhalterzeichen (`*`) für die unbekannten Teile von. ARN Beispiel, `arn:aws:social-messaging:*:`*`123456789012`*`:*`.

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

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

Das folgende Beispiel zeigt, wie Sie die Kontextschlüssel `aws:SourceArn` und `aws:SourceAccount` globale Bedingungskontextschlüssel in Social Messaging verwenden können, um das Confused-Deputy-Problem 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 enthält 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 AWS SMS -Ressourcen verwaltet, einschließlich Sie selbst. Verwenden Sie AWS keine-Root-Anmeldeinformationen zum Verwalten von AWS SMS -Ressourcen.
- Gewähren Sie jedem Benutzer nur den Mindestsatz an Berechtigungen, die für die Ausführung seiner Aufgaben erforderlich sind.
- Verwenden Sie IAM IAM-Gruppen, um Berechtigungen für mehrere Benutzer effektiv zu verwalten.
- Wechseln Sie regelmäßig die IAM-Anmeldeinformationen.

Verwenden von serviceverknüpften AWS Rollen für Amazon

AWS End User Messaging Social verwendet AWS Identity and Access Management (IAM) dienstbezogene Rollen. Eine serviceverknüpfte Rolle ist ein spezieller IAM Rollentyp, der direkt mit AWS End User Messaging Social verknüpft ist. Serviceverknüpfte Rollen werden von AWS End User Messaging Social vordefiniert und schließen alle Berechtigungen ein, die der Service zum Aufrufen anderer AWS -Services in Ihrem Namen erfordert.

Eine serviceverknüpfte Rolle vereinfacht das Einrichten von AWS End User Messaging Social, da Sie die erforderlichen Berechtigungen nicht manuell hinzufügen müssen. AWS End User Messaging Social definiert die Berechtigungen seiner mit dem Service verbundenen Rollen, und sofern nicht anders definiert, kann nur AWS End User Messaging Social seine 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. Dies schützt Ihre AWS End User Messaging Social-Ressourcen, da Sie die Berechtigung für den Zugriff auf die Ressourcen nicht versehentlich entfernen können.

Informationen zu anderen Services, die serviceverknüpfte Rollen unterstützen, finden Sie unter AWS -Services, die mit IAM Featureieren. Suchen Sie nach den Services, für die Yes (Ja) in der Spalte Serviceverknüpfte Rollen angegeben ist. Wählen Sie über einen Link Ja aus, um die Dokumentation zu einer serviceverknüpften Rolle für diesen Service anzuzeigen.

Berechtigungen von serviceverknüpften Rollen AWS für Amazon Notification

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 AWSServiceRoleForSocialMessaging serviceverknüpfte Rolle vertraut darauf, dass die folgenden Services die Rolle übernehmen:

- `social-messaging.amazonaws.com`

Die genannte Richtlinie für Rollenberechtigungen AWSSocialMessagingServiceRolePolicy erlaubt AWS End User Messaging Social die Durchführung der folgenden Aktionen für die angegebenen Ressourcen:

- 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 im IAMBenutzerhandbuch unter Dienstbezogene Rollenberechtigungen.

Aktualisierungen der Richtlinie finden Sie unterAWS Aktualisierungen der AWS verwalteten Richtlinien in Form von End User Messaging Social.

Erstellen einer serviceverknüpften AWS Rolle für Amazon

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

Bearbeiten einer serviceverknüpften AWS Rolle für Amazon

AWS End User Messaging Social erlaubt es Ihnen nicht, die AWSServiceRoleForSocialMessaging serviceverknüpfte Rolle zu 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 bearbeitenIAM. Weitere Informationen finden Sie im IAMBenutzerhandbuch unter Bearbeiten einer dienstbezogenen Rolle.

Löschen einer serviceverknüpften AWS Rolle für Amazon

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 Service AWS End User Messaging Social die Rolle verwendet, wenn Sie versuchen, die Ressourcen zu löschen, schlägt der Löschvorgang 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 AWSServiceRoleForSocialMessaging

1. Rufen Sie `list-linked-whatsapp-business-accounts` API an, um zu erfahren, welche Ressourcen Sie haben.

2. Rufen Sie für jedes verknüpfte Whats App-Geschäftskonto den auf, `disassociate-whatsapp-business-account` API um die Ressource aus dem SocialMessaging Dienst zu entfernen.
3. Stellen Sie sicher, dass keine Ressourcen zurückgegeben wurden, indem Sie den `list-linked-whatsapp-business-accounts` API erneut aufrufen.

So löschen Sie die serviceverknüpfte Rolle mit IAM

Verwenden Sie die IAM Konsole, den oder AWS CLI, AWS API um die AWSServiceRoleForSocialMessaging dienstverknüpfte Rolle zu löschen. Weitere Informationen finden Sie im IAMBenutzerhandbuch unter Löschen einer dienstbezogenen Rolle.

Unterstützte Regionen AWS für serviceverknüpfte Rollen

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

Kontingente für AWS Endbenutzer-Messaging Social

Ihr 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.

Um die Kontingente für AWS End User Messaging Social anzuzeigen, öffnen Sie die Service Quotas Konsole. Wählen Sie im Navigationsbereich AWSDienste und anschließend AWS End User Messaging Social aus.

Informationen zur Erhöhung eines Kontingents finden Sie unter Anfordern einer Kontingenterhöhung im Benutzerhandbuch zu Service Quotas. Wenn das Kontingent unter Service Quotas noch nicht in verfügbar ist, verwenden Sie das Formular zur Erhöhung des Service-Limits.

Ihr AWS -Konto verfügt über die folgenden Kontingente in Bezug auf 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 API aus an das AWS End User Messaging Social richten können AWS-Konto.

Operation	Rate (Tarif)
SendWhatsAppMessage	1.000
PostWhatsAppMessageMedia	100
GetWhatsAppMessageMedia	100
DeleteWhatsAppMessageMedia	100
DisassociateWhatsAppBusinessAccount	10
ListWhatsAppBusinessAccount	10

Operation	Rate (Tarif)
TagResource	10
UntagResourceRate	10
ListTagsForResourceRate	10

Dokumentenverlauf für das AWS End User Messaging Social User Guide

Die folgende Tabelle beschreibt die Dokumentationsversionen für diese AWS Version von Windows Web.

Änderung	Beschreibung	Datum
Erstversion	Erste Version des Benutzerleitfadens für AWS Endbenutzer Messaging Social	10. Oktober Januar

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.