aws

Panduan Pengguna

AWS Pesan Pengguna Akhir Sosial

AWS Pesan Pengguna Akhir Sosial: Panduan Pengguna

Table of Contents

Apa itu AWS End User Messaging Social?

AWS End User Messaging Social, juga disebut sebagai Social messaging, adalah layanan pesan yang memungkinkan pengembang untuk berintegrasi WhatsApp ke dalam aplikasi mereka. Ini menyediakan akses ke WhatsApp kemampuan pesan yang kaya, memungkinkan pembuatan konten interaktif bermerek dengan gambar, video, dan tombol. Dengan menggunakan layanan ini, Anda dapat menambahkan fungsionalitas WhatsApp pesan ke aplikasi Anda bersama saluran yang ada seperti SMS dan pemberitahuan push, memungkinkan Anda untuk terlibat dengan pelanggan melalui saluran komunikasi pilihan mereka.

Untuk memulai, Anda dapat membuat Akun WhatsApp Bisnis baru (WABA) menggunakan proses orientasi mandiri di konsol Sosial Pesan Pengguna AWS Akhir atau menautkan yang sudah ada WABA ke layanan.

Topik

Apakah Anda pengguna baru AWS End User Messaging Social?

Jika Anda pengguna baru AWS End User Messaging Social, sebaiknya mulai dengan membaca bagian berikut:

- Menyiapkan AWS End User Messaging Sosial
- Memulai dengan AWS End User Messaging Social
- Praktik terbaik untuk AWS End User Messaging Sosial

Fitur dari AWS End User Messaging Social

AWS End User Messaging Social menyediakan fitur dan kemampuan berikut:

- Rancang pesan yang konsisten dan gunakan kembali konten secara lebih efektif dengan membuat dan menggunakan templat pesan. Template pesan berisi konten dan pengaturan yang ingin Anda gunakan kembali dalam pesan yang Anda kirim.
- Akses ke kemampuan pesan kaya baru untuk pengalaman yang lebih menarik. Di luar teks dan media Anda dapat mengirim lokasi dan pesan interaktif.
- Terima pesan teks dan media yang masuk dari pelanggan Anda.
- Bangun kepercayaan dengan pelanggan Anda dengan memverifikasi identitas bisnis Anda melalui Meta.

Layanan terkait

AWS menawarkan layanan pesan lain yang dapat digunakan bersama dalam alur kerja multi-saluran:

- Menggunakan AWS End User Messaging SMS untuk mengirim SMS pesan
- Gunakan AWS End User Messaging Push untuk mengirim pemberitahuan push
- Gunakan Amazon SES untuk mengirim email

Mengakses Pesan Pengguna AWS Akhir Sosial

Anda dapat mengakses AWS End User Messaging Social menggunakan berikut ini:

AWS Pesan Pengguna Akhir Konsol Sosial

Antarmuka web tempat Anda membuat dan mengelola sumber daya.

AWS Command Line Interface

Berinteraksi dengan AWS layanan menggunakan perintah di shell baris perintah Anda. AWS Command Line Interface didukung di Windows, macOS, dan Linux. Untuk informasi selengkapnya tentang AWS CLI, lihat Panduan AWS Command Line Interface Pengguna. Anda dapat menemukan AWS SMS perintah di Referensi AWS CLI Perintah.

AWS SDKs

Jika Anda pengembang perangkat lunak yang lebih memilih untuk membangun aplikasi menggunakan bahasa tertentu APIs alih-alih mengirimkan permintaan melalui HTTP atauHTTPS, AWS menyediakan pustaka, kode sampel, tutorial, dan sumber daya lainnya. Pustaka ini menyediakan fungsi dasar yang mengotomatiskan tugas, seperti menandatangani permintaan

Anda secara kriptografis, mencoba kembali permintaan, dan menangani respons kesalahan. Fungsi-fungsi ini membantu membuatnya lebih efisien bagi Anda untuk memulai. Untuk informasi lebih lanjut, lihat Alat untuk Membangun di AWS.

Ketersediaan wilayah

AWS End User Messaging Social tersedia Wilayah AWS dalam beberapa di Amerika Utara, Eropa, Asia, dan Oseania. Di setiap Wilayah, AWS mempertahankan beberapa Availability Zone. Availability Zone ini secara fisik terisolasi satu sama lain, tetapi disatukan oleh koneksi jaringan privat, latensi rendah, throughput tinggi, dan sangat redundan. Availability Zone ini digunakan untuk menyediakan tingkat ketersediaan dan redundansi yang sangat tinggi, sekaligus meminimalkan latensi.

Untuk mempelajari selengkapnya Wilayah AWS, lihat Menentukan Wilayah AWS akun mana yang dapat digunakan di Referensi Umum Amazon Web. Untuk daftar semua Wilayah di mana Sosial Pesan Pengguna AWS Akhir saat ini tersedia dan titik akhir untuk setiap Wilayah, lihat Titik akhir dan kuota untuk AWS End User Messaging Social API dan titik akhir AWS layanan di Referensi Umum Amazon Webatau tabel berikut. Untuk mempelajari selengkapnya tentang jumlah Availability Zone yang tersedia di setiap Wilayah, lihat infrastruktur AWS global.

Ketersediaan wilayah

Nama Wilayah	Wilayah	Titik akhir	WhatsApp APIversi
US East (Northern 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	Versi 20 dan yang lebih baru
AS Timur (Ohio)	us-east-2	social-messaging.us-east-2.amazonaws.com social-messaging-fips.us-east-2.api.aws	Versi 20 dan yang lebih baru

Nama Wilayah	Wilayah	Titik akhir	WhatsApp APIversi
		social-messaging.us-east-2.api.aws	
AS Barat (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	Versi 20 dan yang lebih baru
Asia Pasifik (Mumbai)	ap-south-1	social-messaging.ap-south-1.amazonaws.com social-messaging.ap-south-1.api.aws	Versi 20 dan yang lebih baru
Asia Pasifik (Singapura)	ap-southeast-1	social-messaging.ap-southeast-1.amazonaws.com social-messaging.ap-southeast-1.api.aws	Versi 20 dan yang lebih baru
Eropa (Irlandia)	eu-west-1	social-messaging.eu-west-1.amazonaws.com social-messaging.eu-west-1.api.aws	Versi 20 dan yang lebih baru

Nama Wilayah	Wilayah	Titik akhir	WhatsApp APIversi
Eropa (London)	eu-west-2	social-messaging.eu-west-2.amazonaws.com social-messaging.eu-west-1.api.aws	Versi 20 dan yang lebih baru

Menyiapkan AWS End User Messaging Sosial

Sebelum Anda dapat menggunakan AWS End User Messaging Social untuk pertama kalinya, Anda harus menyelesaikan langkah-langkah berikut.

Topik

Mendaftar Akun AWS

Jika Anda tidak memiliki Akun AWS, selesaikan langkah-langkah berikut untuk membuatnya.

Untuk mendaftar Akun AWS

1. Buka https://portal.aws.amazon.com/billing/pendaftaran.
2. Ikuti petunjuk online.

   Bagian dari prosedur pendaftaran melibatkan tindakan menerima panggilan telepon dan memasukkan kode verifikasi di keypad telepon.

   Saat Anda mendaftar untuk sebuah Akun AWS, sebuah Pengguna root akun AWSdibuat. Pengguna root memiliki akses ke semua Layanan AWS dan sumber daya di akun. Sebagai praktik keamanan terbaik, tetapkan akses administratif ke pengguna, dan gunakan hanya pengguna root untuk melakukan tugas yang memerlukan akses pengguna root.

AWS mengirim Anda email konfirmasi setelah proses pendaftaran selesai. Anda dapat sewaktu-waktu melihat aktivitas akun Anda saat ini dan mengelola akun Anda dengan https://aws.amazon.commengunjungi dan memilih Akun Saya.

Buat pengguna dengan akses administratif

Setelah Anda mendaftar Akun AWS, amankan Pengguna root akun AWS, aktifkan AWS IAM Identity Center, dan buat pengguna administratif sehingga Anda tidak menggunakan pengguna root untuk tugas sehari-hari.

Mengamankan Anda Pengguna root akun AWS

1. Masuk AWS Management Consolesebagai pemilik akun dengan memilih Pengguna root dan memasukkan alamat Akun AWS email Anda. Di laman berikutnya, masukkan kata sandi.

   Untuk bantuan masuk dengan menggunakan pengguna root, lihat Masuk sebagai pengguna root di AWS Sign-In Panduan Pengguna.
2. Mengaktifkan autentikasi multi-faktor (MFA) untuk pengguna root Anda.

   Untuk petunjuk, lihat Mengaktifkan MFA perangkat virtual untuk pengguna Akun AWS root (konsol) Anda di Panduan IAM Pengguna.

Buat pengguna dengan akses administratif

1. Aktifkan Pusat IAM Identitas.

   Untuk mendapatkan petunjuk, silakan lihat Mengaktifkan AWS IAM Identity Center di Panduan Pengguna AWS IAM Identity Center .
2. Di Pusat IAM Identitas, berikan akses administratif ke pengguna.

   Untuk tutorial tentang menggunakan Direktori Pusat Identitas IAM sebagai sumber identitas Anda, lihat Mengkonfigurasi akses pengguna dengan default Direktori Pusat Identitas IAM di Panduan AWS IAM Identity Center Pengguna.

Masuk sebagai pengguna dengan akses administratif

- Untuk masuk dengan pengguna Pusat IAM Identitas, gunakan login URL yang dikirim ke alamat email saat Anda membuat pengguna Pusat IAM Identitas.

  Untuk bantuan masuk menggunakan pengguna Pusat IAM Identitas, lihat Masuk ke portal AWS akses di Panduan AWS Sign-In Pengguna.

Tetapkan akses ke pengguna tambahan

1. Di Pusat IAM Identitas, buat set izin yang mengikuti praktik terbaik menerapkan izin hak istimewa paling sedikit.

   Untuk petunjuknya, lihat Membuat set izin di Panduan AWS IAM Identity Center Pengguna.

2. Tetapkan pengguna ke grup, lalu tetapkan akses masuk tunggal ke grup.

   Untuk petunjuk, lihat Menambahkan grup di Panduan AWS IAM Identity Center Pengguna.

Langkah selanjutnya

Setelah Anda siap bekerja dengan AWS End User Messaging Social, lihat Memulai dengan AWS End User Messaging Social untuk membuat Akun WhatsApp Bisnis (WABA) atau memigrasi Akun WhatsApp Bisnis yang sudah ada.

Memulai dengan AWS End User Messaging Social

Topik ini memandu Anda melalui langkah-langkah untuk menautkan atau memigrasikan Akun WhatsApp Bisnis Anda (WABA) ke AWS End User Messaging Social.

Topik

Daftar untuk WhatsApp

Akun WhatsApp Bisnis (WABA) memungkinkan bisnis Anda menggunakan Platform WhatsApp Bisnis untuk mengirim pesan langsung ke pelanggan Anda. Semua Anda WABAs adalah bagian dari portofolio bisnis Meta Anda. A WABA berisi aset yang dihadapi pelanggan Anda, seperti nomor telepon, templat, dan Profil WhatsApp Bisnis. Profil WhatsApp Bisnis berisi informasi kontak bisnis Anda yang dilihat pengguna. Untuk informasi selengkapnya tentang Akun WhatsApp Bisnis, lihatWhatsApp Akun Bisnis (WABA) di Sosial Pesan Pengguna AWS Akhir.

Ikuti langkah-langkah di bagian ini untuk mulai menggunakan AWS End User Messaging Social. Gunakan proses pendaftaran yang disematkan untuk membuat Akun WhatsApp Bisnis baru (WABA) atau memigrasikan Social Pesan Pengguna AWS Akhir WABA yang sudah ada.

Prasyarat

Important

Bekerja dengan Meta/ WhatsApp

- Penggunaan Solusi WhatsApp Bisnis oleh Anda tunduk pada syarat dan ketentuan Ketentuan Layanan WhatsApp Bisnis, Ketentuan Solusi WhatsApp Bisnis, Kebijakan Pesan WhatsApp Bisnis, Pedoman Pesan, dan semua syarat, kebijakan, atau pedoman lain yang disertakan di dalamnya dengan referensi (karena masing-masing dapat diperbarui dari waktu ke waktu). WhatsApp
- Meta atau WhatsApp dapat sewaktu-waktu melarang penggunaan Solusi WhatsApp Bisnis oleh Anda.
- Anda harus membuat Akun WhatsApp Bisnis (WABA“”) dengan Meta dan WhatsApp.

- Anda harus membuat akun Manajer Bisnis dengan Meta dan menautkannya ke akun AndaWABA.
- Anda harus memberikan kendali Anda WABA kepada kami. Atas permintaan Anda, kami akan mentransfer kendali atas WABA punggung Anda kepada Anda secara wajar dan tepat waktu menggunakan metode yang disediakan Meta bagi kami.
- Sehubungan dengan penggunaan Solusi WhatsApp Bisnis oleh Anda, Anda tidak akan mengirimkan konten, informasi, atau data apa pun yang tunduk pada pengamanan dan/atau pembatasan distribusi sesuai dengan hukum dan/atau peraturan yang berlaku.
- WhatsAppHarga untuk penggunaan Solusi WhatsApp Bisnis dapat ditemukan di Harga Berbasis Percakapan.

- Untuk membuat Akun WhatsApp Bisnis (WABA), bisnis Anda memerlukan Akun Bisnis Meta. Periksa apakah perusahaan Anda sudah memiliki Akun Bisnis Meta. Jika Anda tidak memiliki Akun Meta, Anda dapat membuatnya selama proses pendaftaran.
- Untuk menggunakan nomor telepon yang sudah digunakan dengan aplikasi WhatsApp Messenger atau aplikasi WhatsApp Bisnis, Anda harus menghapusnya terlebih dahulu.
- Nomor telepon yang dapat menerima salah satu SMS atau suara One-Time Passcode ()OTP. Nomor telepon yang digunakan untuk pendaftaran menjadi terkait dengan WhatsApp akun Anda dan nomor telepon digunakan saat Anda mengirim pesan. Nomor telepon masih dapat digunakan untukSMS,MMS, dan pesan suara.
- Jika Anda mengimpor yang sudah adaWABA, Anda memerlukan PINs untuk semua nomor telepon yang terkait dengan imporWABA. Untuk mengatur ulang yang hilang atau terlupakanPIN, ikuti petunjuk dalam Memperbarui PIN di APIReferensi Cloud Platform WhatsApp Bisnis.

Daftar melalui konsol

Ikuti petunjuk berikut untuk membuat WhatsApp akun baru, memigrasi akun yang sudah ada, atau menambahkan nomor telepon ke akun yang sudah adaWABA. Sebagai bagian dari proses pendaftaran, Anda memberikan akses Sosial Pesan Pengguna AWS Akhir ke Akun WhatsApp Bisnis Anda. Anda juga mengizinkan AWS End User Messaging Social untuk menagih Anda untuk pesan. Untuk informasi selengkapnya tentang Akun WhatsApp Bisnis, lihatMemahami jenis akun WhatsApp bisnis.

1. Buka konsol Sosial Pesan Pengguna AWS Akhir di https://console.aws.amazon.com/social-messaging/.
2. Pilih akun Bisnis.
3. Pada halaman Tautkan akun bisnis, pilih Luncurkan portal Facebook. Jendela login baru dari Meta akan muncul.
4. Di jendela login Meta, masukkan kredenal akun Facebook Anda.

   Pada halaman akun WhatsApp bisnis, pilih Tambahkan nomor WhatsApp telepon. Pada halaman Tambahkan nomor WhatsApp telepon, pilih Luncurkan portal Facebook. Jendela login baru dari Meta akan muncul.
5. Di jendela login Meta, masukkan kredenal akun Facebook Anda.
6. Sebagai bagian dari proses pendaftaran, Anda memberikan akses Sosial Pesan Pengguna AWS Akhir ke Akun WhatsApp Bisnis Anda (WABA). Anda juga mengizinkan AWS End User Messaging Social untuk menagih Anda untuk pesan. Pilih Lanjutkan.
7. Untuk akun Meta Business, pilih akun bisnis Meta yang ada atau Buat akun Meta Business.

   a. (Opsional) Jika Anda perlu membuat akun Meta Business, ikuti langkah-langkah ini:

   b. Untuk nama Bisnis, masukkan nama bisnis Anda.

   c. Untuk situs web Bisnis atau halaman profil, masukkan situs web URL untuk perusahaan Anda, atau jika perusahaan Anda tidak memiliki situs web, masukkan URL ke halaman media sosial Anda.

   d. Untuk Negara, pilih negara tempat bisnis Anda berada.

   e. (Opsional) Pilih Tambahkan alamat dan masukkan alamat bisnis Anda.
8. Pilih Berikutnya.
9. Untuk Memilih Akun WhatsApp Bisnis, pilih Akun WhatsApp Bisnis (WABA) yang sudah ada, atau jika Anda perlu membuat akun, pilih Buat Akun WhatsApp Bisnis.

   Untuk Membuat atau Memilih Profil WhatsApp Bisnis, pilih profil WhatsApp bisnis yang ada, atau Buat Profil WhatsApp Bisnis baru.
10. Pilih Berikutnya.
11. Untuk Membuat Profil Bisnis, masukkan informasi berikut:

    - Untuk Nama Akun WhatsApp Bisnis, masukkan nama untuk akun Anda. Bidang ini tidak dihadapi pelanggan.

- Untuk nama tampilan Profil WhatsApp Bisnis, masukkan nama yang akan ditampilkan kepada pelanggan Anda saat mereka menerima pesan dari Anda. Kami merekomendasikan agar Anda menggunakan nama perusahaan Anda. Nama ditinjau oleh Meta dan harus mematuhi aturan nama WhatsApp tampilan. Untuk menggunakan nama merek yang berbeda dari nama perusahaan Anda, harus ada asosiasi yang dipublikasikan secara eksternal antara perusahaan Anda dan merek. Asosiasi ini harus ditampilkan di situs web Anda dan pada merek yang diwakili oleh situs web nama tampilan.

  Setelah Anda menyelesaikan pendaftaran, Meta melakukan peninjauan nama tampilan Anda. Meta mengirimi Anda email yang memberi tahu Anda apakah nama tampilan telah disetujui atau ditolak. Jika nama tampilan Anda ditolak, batas pesan per hari Anda diturunkan dan Anda dapat terputus. WhatsApp

  > **Important**
  >
  > Untuk mengubah nama tampilan Anda, Anda harus membuat tiket dengan dukungan Meta.

- Untuk Timezone, pilih zona waktu tempat bisnis berada.
- Untuk Kategori, pilih kategori yang paling sesuai dengan bisnis Anda. Pelanggan dapat melihat kategori Anda sebagai bagian dari informasi kontak Anda.
- Untuk Deskripsi Bisnis, masukkan deskripsi perusahaan Anda. Pelanggan dapat melihat deskripsi bisnis Anda sebagai bagian dari informasi kontak Anda.
- Untuk Situs Web, masukkan situs web perusahaan Anda. Pelanggan dapat melihat situs web Anda sebagai bagian dari informasi kontak Anda.
- Pilih Berikutnya.

12. Untuk Tambahkan nomor telepon untuk WhatsApp, masukkan nomor telepon untuk mendaftar. Nomor telepon ini ditampilkan kepada pelanggan Anda saat Anda mengirimi mereka pesan.
13. Untuk Pilih cara memverifikasi nomor Anda, pilih Pesan teks atau Panggilan telepon.

    - Setelah Anda siap menerima kode verifikasi, pilih Berikutnya.
    - Masukkan kode verifikasi, lalu pilih Berikutnya.

14. Setelah nomor Anda telah diverifikasi, Anda dapat memilih Berikutnya untuk menutup jendela dari Meta.
15. Untuk akun WhatsApp bisnis, perluas Tag - opsional untuk menambahkan tag ke akun WhatsApp bisnis Anda.

Tag adalah pasangan kunci dan nilai yang dapat Anda terapkan secara opsional ke AWS sumber daya Anda untuk mengontrol akses atau penggunaan. Pilih Tambahkan tag baru dan masukkan pasangan nilai kunci untuk dilampirkan.

16. Akun WhatsApp Bisnis dapat memiliki satu pesan dan tujuan acara untuk mencatat peristiwa untuk Akun WhatsApp Bisnis dan semua sumber daya yang terkait dengan Akun WhatsApp Bisnis. Untuk mengaktifkan pencatatan peristiwa di AmazonSNS, termasuk pencatatan menerima pesan pelanggan, Anda harus mengaktifkan Pesan dan penerbitan acara. Untuk informasi selengkapnya, lihat Tujuan pesan dan acara di AWS End User Messaging Social.

> **Important**
>
> Untuk dapat menanggapi pesan pelanggan, Anda harus mengaktifkan Pesan dan penerbitan acara.

Di bagian Detail tujuan pesan dan acara, aktifkan Penerbitan acara. Untuk AmazonSNS, pilih salah satu topik SNS standar Amazon Baru dan masukkan nama di nama Topik, atau pilih topik SNS standar Amazon yang ada dan pilih topik dari daftar tarik-turun Topik arn.

17. Di bawah nomor Telepon:

    Untuk setiap nomor telepon di bawah Nomor WhtsApp telepon:

    a. Untuk verifikasi nomor telepon, masukkan yang sudah ada PIN atau masukkan PIN kode baru. Untuk mengatur ulang yang hilang atau terlupakanPIN, ikuti petunjuk dalam Memperbarui PIN di APIReferensi Cloud Platform WhatsApp Bisnis.

    b. Untuk pengaturan tambahan:

        i. Untuk wilayah lokalisasi data - opsional pilih salah satu wilayah Meta untuk menyimpan data Anda saat istirahat. Untuk informasi selengkapnya tentang kebijakan privasi data Meta, lihat Privasi & Keamanan Data dan Penyimpanan API Lokal Cloud di APIReferensi Cloud Platform WhatsApp Bisnis.

        ii. Tag adalah pasangan kunci dan nilai yang dapat Anda terapkan secara opsional ke AWS sumber daya Anda untuk mengontrol akses atau penggunaan. Pilih Tambahkan tag baru dan masukkan pasangan nilai kunci untuk dilampirkan.

18. Akun WhatsApp Bisnis dapat memiliki satu pesan dan tujuan acara untuk mencatat peristiwa untuk Akun WhatsApp Bisnis dan semua sumber daya yang terkait dengan Akun WhatsApp

Bisnis. Untuk mengaktifkan pencatatan peristiwa di AmazonSNS, termasuk pencatatan penerimaan pesan pelanggan, Anda harus mengaktifkan Pesan dan penerbitan acara. Untuk informasi selengkapnya, lihat Tujuan pesan dan acara di AWS End User Messaging Social.

> **Important**
>
> Anda harus mengaktifkan Pesan dan penerbitan acara untuk dapat menanggapi pesan pelanggan.

Di bagian Detail tujuan pesan dan acara, aktifkan Penerbitan acara. Untuk AmazonSNS, pilih salah satu topik SNS standar Amazon Baru dan masukkan nama di nama Topik, atau pilih topik SNS standar Amazon yang ada dan pilih topik dari daftar tarik-turun Topik arn.

19. Untuk menyelesaikan pengaturan, pilih Tambahkan nomor telepon.

Langkah selanjutnya

Setelah selesai mendaftar, Anda dapat mulai mengirim pesan. Saat Anda siap untuk mulai mengirim pesan dalam skala besar, selesaikan Verifikasi Bisnis. Setelah akun Sosial Akun WhatsApp Bisnis dan Pesan Pengguna AWS Akhir Anda ditautkan, lihat topik berikut:

- Pelajari tentang tujuan acara untuk mencatat peristiwa dan menerima pesan masuk.
- Pelajari cara membuat templat pesan.
- Pelajari cara mengirim pesan teks atau media.
- Pelajari cara menerima pesan.
- Pelajari tentang Akun Bisnis Resmi untuk memiliki tanda centang hijau di samping nama tampilan Anda dan meningkatkan throughput pesan Anda.

WhatsApp Akun Bisnis (WABA) di Sosial Pesan Pengguna AWS Akhir

Akun WhatsApp Bisnis (WABA) memungkinkan bisnis Anda menggunakan Platform WhatsApp Bisnis untuk mengirim pesan langsung ke pelanggan Anda. Semua Anda WABAs adalah bagian dari Portofolio Bisnis Meta Anda. Akun WhatsApp Bisnis berisi aset yang dihadapi pelanggan Anda seperti nomor telepon, templat, dan informasi kontak bisnis. A hanya WABA bisa ada dalam satu Wilayah AWS. Untuk informasi selengkapnya tentang Akun WhatsApp Bisnis, lihat Akun WhatsApp WhatsApp Bisnis di API Referensi Cloud Platform Bisnis.

Important

Bekerja dengan Meta/ WhatsApp

- Penggunaan Solusi WhatsApp Bisnis oleh Anda tunduk pada syarat dan ketentuan Ketentuan Layanan WhatsApp Bisnis, Ketentuan Solusi WhatsApp Bisnis, Kebijakan Pesan WhatsApp Bisnis, Pedoman Pesan, dan semua syarat, kebijakan, atau pedoman lain yang disertakan di dalamnya dengan referensi (karena masing-masing dapat diperbarui dari waktu ke waktu). WhatsApp
- Meta atau WhatsApp dapat sewaktu-waktu melarang penggunaan Solusi WhatsApp Bisnis oleh Anda.
- Anda harus membuat Akun WhatsApp Bisnis (WABA“”) dengan Meta dan WhatsApp.
- Anda harus membuat akun Manajer Bisnis dengan Meta dan menautkannya ke akun AndaWABA.
- Anda harus memberikan kendali Anda WABA kepada kami. Atas permintaan Anda, kami akan mentransfer kendali atas WABA punggung Anda kepada Anda secara wajar dan tepat waktu menggunakan metode yang disediakan Meta bagi kami.
- Sehubungan dengan penggunaan Solusi WhatsApp Bisnis oleh Anda, Anda tidak akan mengirimkan konten, informasi, atau data apa pun yang tunduk pada pengamanan dan/atau pembatasan distribusi sesuai dengan hukum dan/atau peraturan yang berlaku.
- WhatsAppHarga untuk penggunaan Solusi WhatsApp Bisnis dapat ditemukan di https://developers.facebook.com/docs/whatsapp/harga.

Topik

Melihat Akun WhatsApp Bisnis (WABA) di Sosial Pesan Pengguna AWS Akhir

Ikuti petunjuk ini untuk melihat yang WABA terkait dengan Anda Akun AWS.

1. Buka konsol Sosial Pesan Pengguna AWS Akhir di https://console.aws.amazon.com/social-messaging/.
2. Di akun Bisnis pilih aWABA.
3. Pada tab Nomor telepon, lihat nomor telepon, nama tampilan, peringkat kualitas, dan jumlah percakapan yang dimulai bisnis yang tersisa untuk hari itu.

   Pada tab Tujuan acara, lihat tujuan acara Anda. Untuk mengedit tujuan acara Anda, ikuti petunjuk diTujuan pesan dan acara di AWS End User Messaging Social.

   Pada tab Template pilih Kelola template pesan untuk mengedit WhatsApp template Anda melalui Meta. Masing-masing WABA memiliki batas template 250.

   Pada tab Tag Anda dapat mengelola tag WABA sumber daya Anda.

Menambahkan Akun WhatsApp Bisnis (WABA) di AWS End User Messaging Social

Tambahkan yang baru WABA ke akun Anda jika Anda sudah memiliki Profil WhatsApp Bisnis. Sebagai bagian dari membuat yang baru, WABA Anda harus menambahkan nomor telepon ke fileWABA.

- Untuk menambahkan yang baru WABA ke akun Anda, ikuti langkah-langkah diMemulai dengan AWS End User Messaging Social:
  - Pada langkah 8 pilih Profil WhatsApp Bisnis Anda dan pilih Buat akun WhatsApp Bisnis baru.

Memahami jenis akun WhatsApp bisnis

Akun WhatsApp bisnis Anda menentukan bagaimana penampilan Anda kepada pelanggan Anda. Saat Anda membuat WhatsApp akun, akun Anda akan menjadi Akun Bisnis. WhatsApp Memiliki dua jenis akun Bisnis:

- Akun Bisnis: WhatsApp memverifikasi keaslian setiap akun di Platform WhatsApp Bisnis. Jika akun bisnis telah menyelesaikan proses Verifikasi Bisnis, nama bisnis akan terlihat oleh pengguna meskipun mereka belum menambahkan bisnis ke buku alamat mereka. Fitur ini membantu pengguna mengidentifikasi akun bisnis yang diverifikasi WhatsApp.
- Akun Bisnis Resmi: Seiring dengan manfaat akun bisnis, akun bisnis resmi memiliki lencana tanda centang hijau di profil dan header utas obrolan.

  Persetujuan untuk Akun Bisnis WhatsApp Resmi (OBA) mengharuskan memberikan bukti bahwa bisnis tersebut terkenal dan diakui oleh konsumen, seperti melalui artikel, posting blog, atau ulasan independen. Persetujuan untuk a tidak WhatsApp OBA dijamin, bahkan jika bisnis menyediakan dokumentasi yang diperlukan. Proses persetujuan harus ditinjau dan disetujui oleh WhatsApp. WhatsApp tidak secara terbuka mengungkapkan kriteria spesifik yang mereka gunakan untuk mengevaluasi dan menyetujui aplikasi untuk Akun Bisnis Resmi. Bisnis yang mencari WhatsApp OBA harus menunjukkan reputasi dan pengakuan mereka, tetapi persetujuan akhir adalah kebijaksanaan WhatsApp.

Saat Anda membuat WhatsApp akun, akun Anda akan menjadi Akun Bisnis. Anda dapat memberikan informasi kepada pelanggan Anda tentang bisnis Anda, seperti situs web, alamat, dan jam kerja. Untuk bisnis yang belum menyelesaikan Verifikasi WhatsApp Bisnis, nama tampilan hanya ditampilkan dalam teks kecil di samping nomor telepon dalam tampilan kontak, bukan di daftar obrolan atau obrolan individual. Setelah Verifikasi Bisnis Meta selesai, nama tampilan WhatsApp Pengirim akan ditampilkan di daftar obrolan dan utas obrolan individual.

Sumber daya tambahan

- Untuk informasi selengkapnya tentang Akun Bisnis dan Akun Bisnis Resmi, lihat Akun WhatsApp Bisnis di API Referensi Cloud Platform Bisnis.
- Untuk informasi selengkapnya tentang proses Verifikasi Bisnis, lihat Verifikasi WhatsApp Bisnis di API Referensi Cloud Platform Bisnis.

Nomor telepon di AWS End User Messaging Social

Semua Akun WhatsApp Bisnis berisi satu atau beberapa nomor telepon yang digunakan untuk memverifikasi identitas Anda WhatsApp dan digunakan sebagai bagian dari identitas pengiriman Anda. Anda dapat memiliki beberapa nomor telepon yang terkait dengan Akun WhatsApp Bisnis (WABA) dan menggunakan setiap nomor telepon untuk merek yang berbeda.

Topik

Pertimbangan nomor telepon untuk digunakan dengan Akun WhatsApp Bisnis

Saat Anda menautkan nomor telepon dengan Akun WhatsApp Bisnis Anda (WABA), Anda harus mempertimbangkan hal berikut:

- Nomor telepon hanya dapat ditautkan satu WABA per satu.
- Nomor telepon masih dapat digunakan untukSMS,MMS, dan panggilan suara.
- Setiap nomor telepon memiliki peringkat kualitas dari Meta.

Anda dapat memperoleh nomor telepon SMS berkemampuan melalui AWS End User Messaging SMS dengan melakukan hal berikut:

1. Pastikan bahwa negara atau wilayah untuk nomor telepon mendukung dua arahSMS.
2. Minta nomor telepon. Tergantung pada negara atau wilayah, Anda mungkin diminta untuk mendaftarkan nomor telepon.

3. Aktifkan SMS pesan dua arah untuk nomor telepon. Setelah penyiapan selesai, SMS pesan masuk Anda dikirim ke tujuan acara.

Tambahkan nomor telepon ke Akun WhatsApp Bisnis (WABA)

Anda dapat menambahkan nomor telepon ke Akun WhatsApp Bisnis (WABA) yang sudah ada atau membuat nomor baru WABA untuk nomor telepon.

Prasyarat

Sebelum menggunakan fungsi, prasyarat berikut harus dipenuhi:

- Nomor telepon harus dapat menerima salah satu SMS atau suara One-Time Passcode ()OTP. Ini adalah nomor telepon yang ditambahkan ke AndaWABA.
- Nomor telepon tidak harus dikaitkan dengan yang lainWABA.

Tambahkan nomor telepon ke WABA

Untuk menambahkan nomor telepon baru ke yang sudah ada WABA

1. Buka konsol Sosial Pesan Pengguna AWS Akhir di https://console.aws.amazon.com/social-messaging/.
2. Pilih Akun Bisnis, lalu Tambahkan nomor WhatsApp telepon.
3. Pada halaman Tambahkan nomor WhatsApp telepon, pilih Luncurkan portal Facebook. Jendela login baru dari Meta akan muncul.
4. Di jendela login Meta, masukkan kredenal akun pengembang Meta Anda dan pilih portofolio bisnis Anda.
5. Pilih Profil WhatsApp Bisnis yang ingin Anda tambahkan dengan nomor telepon. WABA
6. Pilih Berikutnya.
7. Untuk Tambahkan nomor telepon untuk WhatsApp, masukkan nomor telepon untuk mendaftar. Nomor telepon ini ditampilkan kepada pelanggan Anda saat Anda mengirimi mereka pesan.
8. Untuk Pilih cara memverifikasi nomor Anda, pilih Pesan teks atau Panggilan telepon.
9. Setelah Anda siap menerima kode verifikasi, pilih Berikutnya
10. Masukkan kode verifikasi, lalu pilih Berikutnya. Setelah nomor Anda telah diverifikasi, Anda dapat memilih Berikutnya untuk menutup jendela dari Meta.

11. Di bawah nomor WhtsApp Telepon:

    a. Untuk verifikasi nomor telepon, masukkan yang sudah ada PIN atau masukkan PIN kode baru. Untuk mengatur ulang yang hilang atau terlupakanPIN, ikuti petunjuk dalam Memperbarui PIN di APIReferensi Cloud Platform WhatsApp Bisnis.

    b. Untuk pengaturan tambahan:

        i. Untuk wilayah lokalisasi data - opsional, pilih salah satu wilayah Meta untuk menyimpan data Anda saat istirahat. Untuk informasi selengkapnya tentang kebijakan privasi data Meta, lihat Privasi & Keamanan Data dan Penyimpanan API Lokal Cloud di APIReferensi Cloud Platform WhatsApp Bisnis.

        ii. Tag adalah pasangan kunci dan nilai yang dapat Anda terapkan secara opsional ke AWS sumber daya Anda untuk mengontrol akses atau penggunaan. Pilih Tambahkan tag baru dan masukkan pasangan nilai kunci untuk dilampirkan.

12. Akun WhatsApp Bisnis dapat memiliki satu pesan dan tujuan acara untuk mencatat peristiwa untuk Akun WhatsApp Bisnis dan semua sumber daya yang terkait dengan Akun WhatsApp Bisnis. Untuk mengaktifkan pencatatan peristiwa di AmazonSNS, termasuk pencatatan penerimaan pesan pelanggan, aktifkan Pesan dan penerbitan acara. Untuk informasi selengkapnya, lihat Tujuan pesan dan acara di AWS End User Messaging Social.

    > **Important**
    >
    > Anda harus mengaktifkan Pesan dan penerbitan acara untuk dapat menanggapi pesan pelanggan.

    Di bagian Detail tujuan pesan dan acara, aktifkan Penerbitan acara. Untuk AmazonSNS, pilih topik SNS standar Amazon Baru dan masukkan nama di Nama topik, atau pilih topik SNSstandar Amazon yang ada dan pilih topik dari daftar tarik-turun Topik arn.

13. Untuk menyelesaikan pengaturan, pilih Tambahkan nomor telepon.

Melihat status nomor telepon

Untuk dapat mengirim pesan di AWS End User Messaging Social, Status nomor telepon harus Aktif.

1. Buka konsol Sosial Pesan Pengguna AWS Akhir di https://console.aws.amazon.com/social-messaging/.

2. Pilih Nomor telepon.
3. Di bagian Nomor telepon, kolom Status memiliki status masing-masing nomor telepon.

> **Note**
>
> Jika Status nomor telepon Penyiapan tidak lengkap, Anda dapat memilih nomor telepon dan kemudian memilih Penyiapan lengkap untuk menyelesaikan pengaturan nomor telepon.

Melihat ID nomor telepon di AWS End User Messaging Social

Untuk dapat mengirim pesan dengan AWS CLI, Anda memerlukan ID nomor telepon untuk mengidentifikasi nomor telepon yang akan digunakan saat mengirim.

1. Buka konsol Sosial Pesan Pengguna AWS Akhir di https://console.aws.amazon.com/social-messaging/.
2. Pilih Nomor telepon.
3. Di bagian Nomor telepon, pilih nomor telepon.
4. Bagian Detail nomor telepon berisi ID nomor telepon dari nomor telepon.

Tingkatkan batas percakapan pesan di WhatsApp

Batas pesan mengacu pada jumlah percakapan maksimum yang dimulai bisnis yang dapat dibuka nomor telepon bisnis dalam periode 24 jam. Nomor telepon bisnis awalnya terbatas pada 250 percakapan yang dimulai bisnis dalam periode bergerak 24 jam. Batas ini dapat ditingkatkan oleh Meta berdasarkan peringkat kualitas pesan Anda dan berapa banyak pesan yang Anda kirim. Percakapan yang diprakarsai bisnis hanya dapat menggunakan pesan template.

Ketika pelanggan mengirim pesan kepada Anda, ini membuka jendela layanan 24 jam. Selama waktu ini, Anda dapat mengirim semua jenis pesan.

Anda dapat meningkatkan batas pesan Anda menjadi 1.000 pesan sendiri dengan mengikuti panduan berikut:

- Nomor telepon bisnis Anda harus memiliki status Aktif.

- Jika nomor telepon bisnis Anda memiliki peringkat kualitas rendah, mungkin terus dibatasi hingga 250 percakapan yang dimulai bisnis per hari hingga peringkat kualitasnya meningkat.
- Mendaftar untuk Verifikasi Bisnis. Jika bisnis Anda disetujui, kualitas pesan akan dianalisis untuk menentukan apakah aktivitas pesan Anda menjamin peningkatan batas pesan Anda. Berdasarkan analisis, permintaan Anda untuk peningkatan batas pesan akan disetujui atau ditolak oleh Meta.
- Ajukan Verifikasi Identitas. Jika Anda menyelesaikan verifikasi identitas dan identitas Anda dikonfirmasi, Meta akan menyetujui peningkatan batas pesan.
- Buka 1.000 atau lebih percakapan yang diprakarsai bisnis dalam periode bergerak 30 hari menggunakan templat dengan peringkat kualitas tinggi. Setelah Anda mencapai ambang 1.000 percakapan, kualitas pesan Anda akan dianalisis untuk menentukan apakah aktivitas pesan Anda menjamin peningkatan batas pesan Anda. Tujuannya adalah untuk mengirim pesan berkualitas tinggi secara konsisten untuk berpotensi meningkatkan batas pesan Anda.

Jika Anda menyelesaikan Verifikasi Bisnis atau Verifikasi Identitas, atau membuka 1.000 percakapan bisnis atau lebih, dan Anda masih terbatas pada 250 percakapan yang dimulai bisnis, kirimkan permintaan ke Meta untuk peningkatan tingkat pesan.

Jika verifikasi bisnis atau identitas Anda ditolak, Anda dapat meningkatkan peluang Anda untuk mendapatkan persetujuan dengan mengirim pesan berkualitas tinggi. Dengan mengirimkan pesan berkualitas tinggi, sesuai, dan opt-in, aktivitas dan kualitas pesan Anda dapat dievaluasi ulang, yang berpotensi mengarah pada peningkatan kemampuan pesan Anda yang disetujui.

Skor kualitas pesan Anda WhatsApp dihitung berdasarkan umpan balik dan interaksi pengguna terbaru, dengan bobot lebih banyak diberikan pada data yang lebih baru. Ini membantu menilai kualitas dan keandalan pesan Anda secara keseluruhan di platform.

Tingkat batas pesan meningkat

- 1K percakapan yang diprakarsai bisnis
- 10K percakapan yang diprakarsai bisnis
- 100 ribu percakapan yang diprakarsai bisnis
- Jumlah percakapan yang diprakarsai bisnis yang tidak terbatas

Tingkatkan throughput pesan di WhatsApp

Throughput pesan adalah jumlah pesan masuk dan keluar per detik (MPS) untuk nomor telepon. Secara default, setiap nomor telepon memiliki MPS 80. Meta dapat meningkatkan Anda MPS menjadi 1.000 jika Anda memenuhi persyaratan berikut:

- Nomor telepon harus dapat mengirim percakapan yang dimulai bisnis dalam jumlah tak terbatas
- Nomor telepon harus memiliki peringkat kualitas sedang atau lebih tinggi.

Memahami peringkat kualitas nomor telepon di WhatsApp

Kualitas nomor telepon dan pesan Anda ditentukan oleh Meta. Skor kualitas pesan Anda didasarkan pada bagaimana pesan Anda telah diterima oleh pelanggan selama 7 hari terakhir, dengan pesan yang lebih baru tertimbang lebih berat. Skor kualitas pesan dihitung berdasarkan kombinasi sinyal kualitas dari percakapan antara Anda dan WhatsApp pengguna Anda. Sinyal ini mencakup umpan balik pengguna seperti blok, laporan, dan alasan yang diberikan pengguna saat mereka memblokir bisnis. Meta mengevaluasi kualitas pesan Anda berdasarkan seberapa baik pesan tersebut diterima oleh pelanggan Anda WhatsApp, dengan fokus pada umpan balik dan interaksi terkini.

WhatsApp Peringkat kualitas nomor telepon

- Hijau: Kualitas tinggi
- Kuning: Kualitas Medium
- Merah: Kualitas rendah

WhatsApp Nomor telepon

- Terhubung: Anda dapat mengirim pesan dalam batas pesan Anda.
- Ditandai: Kualitas nomor telepon Anda rendah dan perlu ditingkatkan. Jika kualitas ponsel Anda tidak membaik dalam 7 hari maka status nomor telepon Anda diubah menjadi Terhubung tetapi batas percakapan yang dimulai bisnis Anda diturunkan satu tingkat.
- Dibatasi: Anda telah mencapai batas percakapan yang dimulai bisnis untuk periode 24 jam saat ini tetapi Anda masih dapat menanggapi pesan pelanggan yang masuk. Setelah periode 24 jam selesai, Anda dapat mengirim pesan lagi.

Melihat peringkat kualitas nomor telepon

Ikuti petunjuk ini untuk melihat kualitas nomor telepon.

1. Buka konsol Sosial Pesan Pengguna AWS Akhir di https://console.aws.amazon.com/social-messaging/.
2. Di akun Bisnis pilih aWABA.
3. Pada tab Nomor telepon, lihat nomor telepon, nama tampilan, peringkat kualitas, dan jumlah percakapan yang dimulai bisnis yang tersisa untuk hari itu.

Menggunakan template pesan di AWS End User Messaging Social

Anda dapat menggunakan templat pesan untuk jenis pesan yang sering Anda gunakan, seperti buletin mingguan atau pengingat janji temu. Pesan template adalah satu-satunya jenis pesan yang dapat dikirim ke pelanggan yang belum mengirim pesan kepada Anda, atau yang belum mengirimi Anda pesan dalam 24 jam terakhir.

Meta memberikan setiap template peringkat kualitas dan status. Peringkat kualitas memengaruhi status template dan menurunkan kecepatan atau kecepatan pengiriman template.

Template dikaitkan dengan Akun WhatsApp Bisnis Anda (WABA), dikelola melalui WhatsApp Manajer, dan ditinjau oleh WhatsApp.

Anda dapat mengirim jenis template berikut:

- Berbasis Teks
- Berbasis media
- Pesan Interaktif
- Berbasis lokasi
- Templat otentikasi dengan tombol kata sandi satu kali
- Template Pesan Multi-Produk

Meta menyediakan templat sampel yang telah disetujui sebelumnya. Untuk mempelajari lebih lanjut, lihat Templat Pesan Contoh.

Untuk informasi selengkapnya tentang jenis templat pesan, lihat Templat pesan di APIReferensi Cloud Platform WhatsApp Bisnis.

Menggunakan template pesan dengan WhatsApp Manajer

Gunakan WhatsAppManajer untuk membuat, memodifikasi, atau memeriksa status templat.

1. Buka konsol Sosial Pesan Pengguna AWS Akhir di https://console.aws.amazon.com/social-messaging/.

2. Pilih akun Bisnis, lalu pilihWABA.
3. Pada tab Templat pesan, pilih Kelola templat pesan. WhatsAppManajer membuka di jendela baru di mana Anda dapat mengelola template Anda dengan memilih Template pesan.

Langkah selanjutnya

Setelah Anda membuat atau mengedit template, Anda harus mengirimkannya untuk ditinjau. WhatsApp Peninjauan Meta dapat memakan waktu hingga 24 jam. Meta mengirimkan email ke admin Manajer Bisnis Anda dan memperbarui status template di WhatsApp manajer. Gunakan WhatsAppmanajer untuk memeriksa status template Anda.

Memahami template mondar-mandir WhatsApp

Template pacing adalah metode, yang digunakan oleh Meta, yang memungkinkan waktu untuk umpan balik pelanggan awal pada template baru atau yang dimodifikasi. Ini mengidentifikasi dan menghentikan template yang menerima keterlibatan atau umpan balik yang buruk, memberi Anda waktu untuk menyesuaikan konten template sebelum mengirimkannya ke terlalu banyak pelanggan. Ini mengurangi risiko umpan balik pelanggan negatif yang berdampak pada bisnis. Misalnya, jika terlalu banyak pelanggan “memblokir” pesan Anda, atau jika template Anda memiliki tingkat baca rendah, maka peringkat kualitas template Anda dapat diturunkan.

Template pacing mempengaruhi template yang baru dibuat, template yang tidak dijeda, dan template tanpa rating berkualitas tinggi. Template pacing sering dimulai dengan riwayat template berkualitas rendah atau dijeda sebelumnya. Ketika template berjalan, pesan yang menggunakan template tersebut dikirim secara normal hingga ambang batas tertentu yang ditentukan oleh Meta. Setelah itu, pesan berikutnya diadakan untuk memberikan waktu untuk umpan balik pelanggan. Jika umpan baliknya positif, mondar-mandir template kemudian ditingkatkan. Jika umpan balik negatif, mondar-mandir template diturunkan, memungkinkan Anda untuk menyesuaikan konten template. Untuk informasi selengkapnya, lihat Template mondar-mandir di APIReferensi Cloud Platform WhatsApp Bisnis.

Dapatkan umpan balik tentang status template yang diturunkan dengan WhatsApp Manajer

Meta memberikan informasi tentang alasan status template diturunkan. Gunakan umpan balik dari Meta untuk mengedit template dan mengirimkannya untuk disetujui kembali, menggunakan

template yang berbeda, atau mengubah perilaku aplikasi Anda. Jika Anda mengedit templat pesan dan disetujui kembali, peringkat kualitasnya akan meningkat secara bertahap selama tidak sering menerima umpan balik negatif atau tingkat baca rendah.

1. Buka konsol Sosial Pesan Pengguna AWS Akhir di https://console.aws.amazon.com/social-messaging/.
2. Pilih akun Bisnis, lalu pilihWABA.
3. Pada tab Templat pesan, pilih Kelola templat pesan. WhatsAppManajer membuka di jendela baru.
4. Pilih template Pesan, dan arahkan kursor ke template. Tooltip akan muncul dengan umpan balik tentang mengapa peringkat diturunkan.

Memahami status template dan peringkat kualitas di WhatsApp

Setiap template pesan diberi peringkat kualitas berdasarkan penggunaan, umpan balik pelanggan, dan keterlibatan pelanggan. Template hanya dapat digunakan jika statusnya Aktif, tetapi kualitasnya menentukan kecepatan template. Jika template pesan secara konsisten menerima umpan balik negatif atau mengalami keterlibatan rendah, itu akan menyebabkan perubahan status template.

Meta mengubah status template atau peringkat kualitas secara otomatis berdasarkan umpan balik dan keterlibatan negatif atau positif. Jika status template Anda berubah, Anda akan menerima pemberitahuan WhatsApp Manajer, email, dan pemberitahuan acara. Gunakan WhatsAppmanajer untuk memeriksa status template Anda.

Jika template Anda ditolak oleh WhatsApp, Anda dapat mengedit template dan mengirim ulang untuk persetujuan atau mengajukan banding WhatsApp. Untuk mempelajari selengkapnya, lihat Banding di APIReferensi Cloud Platform WhatsApp Bisnis.

Status templat	Penilaian kualitas	Arti
Dalam Peninjauan		Template pesan sedang ditinjau. Diperlukan waktu hingga 24 jam agar selesai.
Ditolak		Template pesan ditolak, dan Anda dapat mengajukan banding.

Status templat	Penilaian kualitas	Arti
Aktif	Tertunda	Template pesan belum menerima umpan balik berkualitas atau informasi tingkat baca dari pelanggan , tetapi template masih dapat digunakan untuk mengirim pesan.
Aktif	Tinggi	Template pesan telah menerima sedikit atau tidak ada umpan balik pelanggan negatif dan dapat digunakan untuk mengirim pesan.
Aktif	Sedang	Template pesan telah menerima umpan balik negatif dari pelanggan, atau tingkat baca rendah, dan dapat dijeda atau dimatikan.
Aktif	Rendah	Template pesan telah menerima umpan balik negatif dari pelanggan, atau tingkat baca rendah. Template pesan dengan status ini dapat digunakan, tetapi berisiko dijeda atau dinonaktifkan. Ketika template pindah ke status Active-Low, pengirima nnya dijeda. Jeda pertama adalah tiga jam, jeda kedua adalah enam jam, dan jeda berikutnya menonaktifkan template.

Status templat	Penilaian kualitas	Arti
Dijeda		Template pesan telah dijeda karena umpan balik negatif berulang dari pelanggan, atau tingkat baca yang rendah.
Nonaktif		Template pesan telah dinonaktifkan karena umpan balik negatif berulang dari pelanggan.
Banding Diminta		Banding telah diminta.

Alasan mengapa template ditolak di WhatsApp

Jika template pesan Anda ditinjau dan ditolak oleh Meta, Anda akan menerima email yang menjelaskan mengapa template ditolak. Anda dapat mengajukan banding atas penolakan atau memodifikasi templat pesan Anda. Ini adalah beberapa alasan umum Meta mungkin menolak template pesan:

- Parameter variabel berisi karakter khusus, seperti #, $, atau%.
- Parameter variabel tidak ada, memiliki kurung kurawal yang tidak cocok, atau tidak berurutan.
- Template pesan berisi konten yang melanggar Kebijakan WhatsApp Perdagangan atau Kebijakan WhatsApps Bisnis.

Untuk informasi selengkapnya, lihat Alasan Penolakan Umum di APIReferensi Cloud Platform WhatsApp Bisnis.

Tujuan pesan dan acara di AWS End User Messaging Social

Tujuan peristiwa adalah SNS topik Amazon tempat WhatsApp peristiwa dikirim. Saat Anda mengaktifkan penerbitan acara ke SNS topik Amazon, semua acara kirim dan terima Anda dikirim ke SNS topik Amazon. Gunakan acara untuk memantau, melacak, dan menganalisis status pesan keluar dan komunikasi pelanggan yang masuk.

Setiap Akun WhatsApp Bisnis (WABA) dapat memiliki satu tujuan acara. Semua peristiwa dari semua sumber daya yang terkait dengan Akun WhatsApp Bisnis dicatat ke tujuan acara tersebut. Misalnya, Anda dapat memiliki Akun WhatsApp Bisnis dengan tiga nomor telepon yang terkait dengannya dan semua peristiwa dari nomor telepon tersebut dicatat ke satu tujuan acara.

Topik

Menambahkan pesan dan tujuan acara ke AWS End User Messaging Social

Saat Anda mengaktifkan penerbitan pesan dan acara, semua peristiwa yang dihasilkan oleh Akun WhatsApp Bisnis (WABA) Anda akan dikirim ke SNS topik Amazon. Ini termasuk acara untuk setiap nomor telepon yang terkait dengan Akun WhatsApp Bisnis. Anda WABA dapat memiliki satu SNS topik Amazon yang terkait dengannya.

Prasyarat

Sebelum menggunakan fungsi, prasyarat berikut harus dipenuhi.

- (Opsional) Untuk menggunakan SNS topik Amazon yang dienkripsi menggunakan AWS KMS kunci, Anda harus memberikan izin Sosial Pesan Pengguna AWS Akhir ke kebijakan kunci yang ada.

Menambahkan pesan dan tujuan acara

1. Buka konsol Sosial Pesan Pengguna AWS Akhir di https://console.aws.amazon.com/social-messaging/.
2. Pilih akun Bisnis, lalu pilihWABA.
3. Pada tab Tujuan acara, pilih Edit tujuan.
4. Untuk mengaktifkan tujuan acara, pilih Aktifkan.
5. Untuk mengirim acara Anda ke SNS tujuan Amazon baru, pilih Topik SNS stand baru, dan masukkan nama di Nama topik. SNSTopik Amazon dibuat dengan izin untuk memungkinkan AWS End User Messaging Social mengakses topik.

   Untuk mengirim acara Anda ke SNS tujuan Amazon yang ada, pilih Topik SNS standar yang ada, dan pilih formulir topik topik arn. Anda harus menerapkan izin berikut ke SNS topik Amazon:

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

Kebijakan topik Amazon SNS terenkripsi

Anda dapat menggunakan SNS topik Amazon yang dienkripsi menggunakan AWS KMS kunci untuk tingkat keamanan tambahan. Keamanan tambahan ini dapat membantu jika aplikasi Anda menangani data pribadi atau sensitif. Untuk informasi selengkapnya tentang mengenkripsi SNS topik Amazon menggunakan AWS KMS kunci, lihat Mengaktifkan kompatibilitas antara sumber peristiwa dari AWS layanan dan topik terenkripsi di Panduan Pengembang Layanan Pemberitahuan Sederhana Amazon.

Pernyataan contoh menggunakan, opsional tetapi direkomendasikan, `SourceAccount` dan `SourceArn` kondisi untuk menghindari masalah wakil yang membingungkan dan hanya akun pemilik

AWS End User Messaging Social yang memiliki akses. Untuk informasi lebih lanjut tentang masalah wakil yang bingung, lihat Masalah wakil yang bingung di panduan IAM pengguna.

Kunci yang Anda gunakan harus simetris. SNSTopik Amazon terenkripsi tidak mendukung kunci asimetris AWS KMS .

Kebijakan utama harus dimodifikasi agar AWS End User Messaging Social dapat menggunakan kunci tersebut. Ikuti petunjuk dalam Mengubah kebijakan kunci, di Panduan AWS Key Management Service Pengembang, untuk menambahkan izin berikut ke kebijakan kunci yang ada:

```
{
    "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}:*"
        }
     }
}
```

Langkah selanjutnya

Setelah menyiapkan SNS topik Amazon, Anda harus berlangganan endpoint untuk topik. endpoint akan mulai menerima pesan yang diterbitkan ke topik terkait. Untuk informasi selengkapnya tentang berlangganan topik, lihat Berlangganan SNS topik Amazon di Panduan SNS Pengembang Amazon.

Format pesan dan acara di AWS End User Messaging Social

JSONObjek untuk acara berisi header AWS acara dan WhatsApp JSON payload. Untuk daftar payload dan nilai JSON WhatsApp notifikasi, lihat Referensi Payload Pemberitahuan Webhook dan Status Pesan di Referensi Cloud Platform WhatsApp Bisnis. API

AWS Header acara Sosial Pesan Pengguna Akhir

JSONObjek untuk acara berisi header AWS acara dan WhatsApp JSON. Header berisi AWS pengidentifikasi dan ARNs Akun WhatsApp Bisnis Anda (WABA) dan nomor telepon.

```
{
  "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
}
```

Dalam contoh peristiwa sebelumnya:

- *1234567890abcde* adalah WABA id dari Meta.
- *abcde1234567890* adalah id nomor telepon dari Meta.
- *fb2594b8a7974770b128a409e2example* adalah ID dari Akun WhatsApp Bisnis (WABA).
- *976c72a700aac43eaf573ae050example* adalah ID dari nomor telepon.

Contoh WhatsApp JSON untuk menerima pesan teks

Berikut ini menunjukkan catatan peristiwa untuk pesan teks masuk dari WhatsApp. JSONItu dihasilkan oleh WhatsApp. Untuk daftar bidang dan artinya, lihat Referensi Payload Pemberitahuan Webhook di Referensi Cloud Platform WhatsApp Bisnis. API

```
{
```

```
//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"
    }
  ]
}
```

Contoh WhatsApp JSON untuk menerima pesan media

Berikut ini menunjukkan catatan acara untuk pesan media yang masuk. Untuk mengambil file media, gunakan GetWhatsAppMessageMedia API perintah. Untuk daftar bidang dan artinya, lihat Referensi Payload Pemberitahuan Webhook

```
{
//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 status pesan

Saat mengirim pesan, Anda menerima pembaruan status pesan. Anda harus mengaktifkan pencatatan peristiwa untuk menerima pemberitahuan ini, lihatTujuan pesan dan acara di AWS End User Messaging Social.

Status pesan

Tabel berikut berisi kemungkinan status pesan.

Nama status	Deskripsi
dihapus	Pelanggan menghapus pesan, dan Anda juga harus menghapus pesan jika diunduh ke server Anda.
dikirim	Pesan berhasil dikirim ke pelanggan.
gagal	Pesan gagal dikirim.
baca	Pelanggan membaca pesannya. Status ini hanya dikirim jika pelanggan telah membaca tanda terima dihidupkan.
dikirim	Pesan telah dikirim tetapi masih dalam perjalanan.
memperingati	Pesan berisi item yang tidak tersedia atau tidak ada.

Sumber daya tambahan

Untuk informasi selengkapnya, lihat Status Pesan di APIReferensi Cloud Platform WhatsApp Bisnis.

Mengunggah file media untuk dikirim WhatsApp

Saat Anda mengirim atau menerima file media, file media harus disimpan di bucket Amazon S3. Bucket Amazon S3 harus sama Akun AWS dan Wilayah AWS sebagai Akun WhatsApp Bisnis Anda ()WABA. Petunjuk ini menunjukkan cara membuat bucket Amazon S3, mengunggah file, dan membuat file URL ke file. Untuk informasi selengkapnya tentang perintah Amazon S3, lihat Menggunakan perintah tingkat tinggi (s3) dengan perintah. AWS CLI Untuk informasi selengkapnya tentang mengonfigurasi AWS CLI, lihat Mengonfigurasi AWS CLI di Panduan AWS Command Line Interface Pengguna, dan Membuat bucket, serta Mengunggah objek di Panduan Pengguna Amazon S3.

Anda juga dapat membuat presigned URL ke file media. Dengan presignedURL, Anda dapat memberikan akses terbatas waktu ke objek dan mengunggahnya tanpa memerlukan pihak lain untuk memiliki kredensi atau izin AWS keamanan.

Untuk membuat bucket Amazon S3, gunakan perintah AWS CLI create-bucket. Di baris perintah, masukkan perintah berikut:

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

Dalam perintah sebelumnya:

- Ganti *us-east-1* dengan Wilayah AWS yang Anda WABA ada di dalamnya.
- Ganti *BucketName* dengan nama ember baru.

Untuk menyalin file ke bucket Amazon S3, gunakan perintah cp AWS CLI . Di baris perintah, masukkan perintah berikut:

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

Dalam perintah sebelumnya:

- Ganti *SourceFilePathAndName* dengan jalur file dan nama file yang akan disalin.
- Ganti *BucketName* dengan nama ember.
- Ganti *FileName* dengan nama yang akan digunakan untuk file tersebut.

Url yang digunakan saat mengirim adalah:

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

Untuk membuat presigned URL, ganti *user input placeholders* dengan informasi Anda sendiri.

```
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
```

Yang dikembalikan URL akan menjadi: `https://amzn-s3-demo-bucket1.s3.af-south-1.amazonaws.com/mydoc.txt?{Headers}`

Jenis dan ukuran file media yang didukung di WhatsApp

Saat mengirim atau menerima pesan media, jenis file harus didukung dan di bawah ukuran file maksimum. Untuk informasi selengkapnya, lihat Jenis Media yang Didukung di APIReferensi Cloud Platform WhatsApp Bisnis.

Tipe file media

Format audio

Tipe Audio	Ekstensi	MIMETipe	Ukuran Maks
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

Format dokumen

Tipe Dokumen	Ekstensi	MIMETipe	Ukuran Maks
Teks	.text	teks/polos	100 MB
Microsoft Excel	.xls, .xlsx	aplikasi/vnd.ms-excel, aplikasi/vnd.openx	100 MB

Tipe Dokumen	Ekstensi	MIMETipe	Ukuran Maks
		mlformats-officedocument.spreadsheetml.sheet	
Microsoft Word	.doc, .docx	aplikasi/msword, aplikasi/vnd.openxmlformats-officedocument.wordprocessingml.document	100 MB
Microsoft PowerPoint	.ppt, .pptx	aplikasi/vnd.ms-powerpoint, aplikasi/vnd.openxmlformats-officedocument.presentationml.presentation	100 MB
PDF	.pdf	aplikasi/pdf	100 MB

Format citra

Tipe Citra	Ekstensi	MIMETipe	Ukuran Maks
JPEG	.jpeg	gambar/jpeg	5 MB
PNG	.png	gambar/png	5 MB

Format stiker

Tipe Stiker	Ekstensi	MIMETipe	Ukuran Maks
Stiker animasi	.webp	gambar/webp	500 KB
Stiker statis	.webp	gambar/webp	100 KB

Format video

Tipe video	Ekstensi	MIMETipe	Ukuran Maks
3 GPP	.3gp	Video/3gp	16 MB
MP4Video	.mp4	Video/mp4	16 MB

WhatsApp jenis pesan

Topik ini mencantumkan jenis pesan yang didukung dan deskripsi penggunaannya. Untuk daftar jenis pesan, lihat Pesan di APIReferensi Cloud Platform WhatsApp Bisnis.

Jenis pesan	Deskripsi
Teks	Kirim pesan teks atau URL ke pelanggan Anda
Media	Kirim file audio, dokumen, gambar, stiker, atau video. Anda juga dapat mengirim tautan file media.
Reaksi	Kirim emoji sebagai reaksi terhadap pesan seperti jempol
Templat	Kirim pesan template
Lokasi	Mengirim lokasi
Kontak	Kirim kartu kontak
Interaktif	Kirim pesan interaktif

Sumber daya tambahan

Untuk daftar objek WhatsApp pesan, lihat Pesan di APIReferensi Cloud Platform WhatsApp Bisnis.

Mengirim pesan melalui WhatsApp AWS End User Messaging Social

Sebelum mengirim pesan, Anda harus menyelesaikan pengaturan Anda WABA dan pengguna Anda harus memilih untuk menerima pesan dari Anda, lihat. Mendapatkan izin

Ketika pengguna mengirim pesan kepada Anda, timer 24 jam yang disebut jendela layanan pelanggan dimulai atau disegarkan. Semua jenis pesan, kecuali untuk pesan template, hanya dapat dikirim ke pengguna ketika jendela layanan pelanggan terbuka antara Anda dan pengguna. Pesan template dapat dikirim ke pengguna kapan saja, selama pengguna telah memilih untuk menerima pesan dari Anda.

Untuk setiap pesan yang Anda kirim atau terima, status pesan dibuat dan dikirim ke tujuan acara. Jika pelanggan Anda belum mendaftar untuk WhatsApp acara dihasilkan dengan status pesan`fail`. Anda harus mengaktifkan pesan dan tujuan acara untuk menerima status pesan.

> **Important**
>
> Bekerja dengan Meta/ WhatsApp
>
> - Penggunaan Solusi WhatsApp Bisnis oleh Anda tunduk pada syarat dan ketentuan Ketentuan Layanan WhatsApp Bisnis, Ketentuan Solusi WhatsApp Bisnis, Kebijakan Pesan WhatsApp Bisnis, Pedoman Pesan, dan semua syarat, kebijakan, atau pedoman lain yang disertakan di dalamnya dengan referensi (karena masing-masing dapat diperbarui dari waktu ke waktu). WhatsApp
> - Meta atau WhatsApp dapat sewaktu-waktu melarang penggunaan Solusi WhatsApp Bisnis oleh Anda.
> - Sehubungan dengan penggunaan Solusi WhatsApp Bisnis oleh Anda, Anda tidak akan mengirimkan konten, informasi, atau data apa pun yang tunduk pada pengamanan dan/atau pembatasan distribusi sesuai dengan hukum dan/atau peraturan yang berlaku.

Topik

Contoh pengiriman pesan template di AWS End User Messaging Social

Contoh berikut menunjukkan cara menggunakan template untuk mengirim pesan ke pelanggan Anda menggunakan AWS CLI. Untuk informasi selengkapnya tentang mengonfigurasi AWS CLI, lihat Mengkonfigurasi AWS CLI dalam Panduan AWS Command Line Interface Pengguna.

```
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
```

Pada perintah sebelumnya, lakukan hal berikut:

- Ganti *{PHONE_NUMBER}* dengan nomor telepon pelanggan Anda.
- Ganti *{ORIGINATION_PHONE_NUMBER_ID}* dengan ID nomor telepon Anda.

Contoh pengiriman pesan media di AWS End User Messaging Social

Contoh berikut menunjukkan cara mengirim pesan media ke pelanggan Anda menggunakan pesan media AWS CLI. Untuk informasi selengkapnya tentang mengonfigurasi AWS CLI, lihat Mengkonfigurasi AWS CLI dalam Panduan AWS Command Line Interface Pengguna. Untuk mengetahui daftar jenis file media yang didukung, lihatJenis dan ukuran file media yang didukung di WhatsApp.

1. Unggah file media ke bucket Amazon S3, lihat. Mengunggah file media untuk dikirim WhatsApp
2. Unggah file media untuk WhatsApp menggunakan post-whatsapp-message-mediaperintah. Setelah berhasil menyelesaikan perintah akan mengembalikan *{MEDIA_ID}* yang diperlukan untuk mengirim pesan media.

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

   Pada perintah sebelumnya, lakukan hal berikut:

- Ganti *{ORIGINATION_PHONE_NUMBER_ID}* dengan ID nomor telepon Anda.
- Ganti *{BUCKET}* dengan nama ember Amazon S3.
- Ganti *{MEDIA_FILE}* dengan nama file media.

Anda juga dapat mengunggah menggunakan url presign dengan menggunakan `--source-s3-presigned-url` alih-alih. `--source-s3-file` Anda harus menambahkan `Content-Type` di bidang header. Jika Anda menggunakan keduanya maka `InvalidParameterException` an dikembalikan.

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

3. Gunakan send-whatsapp-messageperintah untuk mengirim pesan media.

```
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
```

Pada perintah sebelumnya, lakukan hal berikut:

- Ganti *{PHONE_NUMBER}* dengan nomor telepon pelanggan Anda.
- Ganti *{ORIGINATION_PHONE_NUMBER_ID}* dengan ID nomor telepon Anda.
- Ganti *{MEDIA_ID}* dengan id media dikembalikan dari langkah sebelumnya.

4. Saat tidak lagi membutuhkan file media, Anda dapat menghapusnya dari WhatsApp menggunakan delete-whatsapp-message-mediaperintah. Ini hanya menghapus file media dari WhatsApp dan bukan bucket Amazon S3 Anda.

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

Pada perintah sebelumnya, lakukan hal berikut:

- Ganti *{ORIGINATION_PHONE_NUMBER_ID}* dengan ID nomor telepon Anda.
- Ganti *{MEDIA_ID}* dengan id media.

Menanggapi pesan yang diterima di AWS End User Messaging Social

Sebelum Anda dapat menerima pesan teks atau media, Anda harus menyelesaikan pengaturan WABA dan pengaturan tujuan acara. Saat Anda menerima pesan masuk, acara disimpan di SNS topik Amazon tujuan acara. Anda harus berlangganan titik akhir SNS topik Amazon untuk menerima pemberitahuan.

Untuk contoh peristiwa pesan media yang diterima, lihatContoh WhatsApp JSON untuk menerima pesan media. Untuk informasi selengkapnya tentang mengonfigurasi AWS CLI, lihat Mengkonfigurasi AWS CLI dalam Panduan AWS Command Line Interface Pengguna. Untuk daftar jenis file media yang didukung, lihatJenis dan ukuran file media yang didukung di WhatsApp.

> **Important**
>
> Untuk menerima pesan masuk, Anda harus mengaktifkan tujuan acaraWABA, lihatMenambahkan pesan dan tujuan acara ke AWS End User Messaging Social.

Contoh mengubah status pesan untuk dibaca dengan AWS End User Messaging Social

Anda dapat mengatur status pesan untuk menunjukkan `read` kepada pengguna akhir dua tanda centang biru di layar mereka.

```
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
```

Pada perintah sebelumnya, lakukan hal berikut:

- Ganti *{ORIGINATION_PHONE_NUMBER_ID}* dengan ID nomor telepon Anda.
- Ganti *{MESSAGE_ID}* dengan pengenal unik pesan. Gunakan nilai `id` bidang di objek pesan SNS topik Amazon.

Contoh menanggapi pesan dengan reaksi di AWS End User Messaging Social

Anda dapat menambahkan reaksi ke pesan, seperti jempol ke atas.

```
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
```

Pada perintah sebelumnya, lakukan hal berikut:

- Ganti *{PHONE_NUMBER}* dengan nomor telepon pelanggan Anda.
- Ganti *{MESSAGE_ID}* dengan pengenal unik pesan. Gunakan nilai `id` bidang di objek pesan SNS topik Amazon.
- Ganti *{ORIGINATION_PHONE_NUMBER_ID}* dengan ID nomor telepon Anda.

Unduh file media dari Amazon S3 WhatsApp ke

Untuk mengambil file media dan menyimpannya ke bucket Amazon S3 gunakan get-whatsapp-message-mediaperintah.

```
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
}
```

Pada perintah sebelumnya, lakukan hal berikut:

- Ganti *{BUCKET}* dengan nama bucket Amazon S3.
- Ganti *{MEDIA_ID}* dengan nilai bidang id dari acara yang diterima. Untuk contoh acara media masuk, lihatContoh WhatsApp JSON untuk menerima pesan media.
- Ganti *{ORIGINATION_PHONE_NUMBER_ID}* dengan ID nomor telepon Anda.

Untuk mengambil media dari bucket Amazon S3 gunakan perintah berikut:

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

Pada perintah sebelumnya, lakukan hal berikut:

- Ganti *{BUCKET}* dengan nama bucket Amazon S3.
- Ganti *{MEDIA_ID}* dengan MEDIA _ID dikembalikan dari langkah sebelumnya.

Contoh menanggapi pesan dengan membaca dan reaksi

Dalam contoh ini, pelanggan Anda, Diego, telah mengirimi Anda pesan yang mengatakan “Hai” dan Anda menanggapinya dengan tanda terima baca dan emoji gelombang tangan.

Prasyarat

Anda harus menyiapkan SNS topik Amazon tujuan acara dan berlangganan salah satu titik akhir topik untuk menerima pemberitahuan bahwa Diego mengirim pesan.

Merespons

1. Ketika pesan dari Diego diterima, sebuah acara dipublikasikan ke titik akhir topik. Berikut ini adalah cuplikan dari apa yang dipublikasikan topik tersebut.

   > **Note**
   >
   > Karena Diego memulai percakapan itu tidak diperhitungkan terhadap percakapan yang dimulai bisnis Anda.

   ```
   {
     "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. Untuk menunjukkan Diego, Anda menerima pesan, atur statusnya. `read` Diego akan melihat dua tanda centang biru di sebelah pesan di perangkatnya.

```
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
```

Pada perintah sebelumnya, lakukan hal berikut:

- Ganti *{ORIGINATION_PHONE_NUMBER_ID}* dengan id nomor telepon yang Diego kirimi pesannya. `phone-number-id-976c72a700aac43eaf573ae050example`
- Ganti *{MESSAGE_ID}* dengan pengenal unik pesan. Ini adalah nilai id yang sama dalam pesan yang diterima`wamid.HBgLMTQyNTY5ODgzMDIVAgASGCBDNzBDRjM5MDU2ODEwMDkwREY4ODBDRDE0RjV`

3. Anda dapat mengirim Diego reaksi gelombang tangan.

```
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
```

Pada perintah sebelumnya, lakukan hal berikut:

- Ganti *{PHONE_NUMBER}* dengan nomor `14255550150` telepon Diego.
- Ganti *{MESSAGE_ID}* dengan pengenal unik pesan. Ini adalah nilai id yang sama dalam pesan yang diterima`wamid.HBgLMTQyNTY5ODgzMDIVAgASGCBDNzBDRjM5MDU2ODEwMDkwREY4ODBDRDE0RjV`
- Ganti *{ORIGINATION_PHONE_NUMBER_ID}* dengan id nomor telepon yang Diego kirimi pesannya. `phone-number-id-976c72a700aac43eaf573ae050example`

Sumber daya tambahan

- Aktifkan tujuan acara untuk mencatat peristiwa dan menerima pesan masuk.
- Untuk daftar objek WhatsApp pesan, lihat Pesan di APIReferensi Cloud Platform WhatsApp Bisnis.

Memahami laporan WhatsApp penagihan dan penggunaan untuk AWS End User Messaging Social

Saluran Sosial Pesan Pengguna AWS Akhir menghasilkan jenis penggunaan yang berisi lima bidang dalam format berikut:*Region code*-*MessagingType*-*ISO*-*FeeDescription*-*FeeType*. Ada dua item penagihan yang mungkin untuk setiap WhatsApp percakapan WhatsApp`ConversationFee`, dan AWS per`MessageFee`.

Ketika Anda memulai percakapan dengan mengirim pesan template, Anda akan ditagih untuk satu WhatsApp `ConversationFee` dan satu AWS per. `MessageFee` Ini membuka jendela 24 jam di mana setiap pesan yang Anda kirim atau terima dari pelanggan yang sama ditagih sebagai AWS per`MessageFee`.

Jenis WhatsApp percakapan dan detail harga dapat ditemukan di Harga Berbasis Percakapan di Panduan Pengembang Platform WhatsApp Bisnis.

Tabel berikut menampilkan nilai dan deskripsi yang mungkin untuk bidang dalam jenis penggunaan. Untuk informasi selengkapnya tentang harga Sosial Pesan Pengguna AWS AWS Akhir, lihat Harga Pesan Pengguna Akhir.

Bidang	Opsi	Deskripsi
Region code	• USE1Wilayah US East (N. Virginia) • USE2— Wilayah US East (Ohio) • USW1— Wilayah US West (Oregon) • APS1Wilayah Asia Pasifik (Mumbai) • APSE1Wilayah Asia Pasifik (Singapura) • EUW1Wilayah Eropa (Irlandia)	Wilayah AWS Awalan yang menunjukkan dari mana WhatsApp pesan dikirim atau diterima.

Bidang	Opsi	Deskripsi
	• EUW2Wilayah Eropa (London)	
MessagingType	`WhatsApp`	Bidang ini mengidentifikasi jenis pesan yang dikirim.
ISO	Lihat negara yang didukung	Kode ISO negara dua digit tempat pesan dikirim.
FeeDescription	`ConversationFee` , `MessageFee`	Bidang ini menentukan baik WhatsApp `ConversationFee` atau AWS per`MessageFee` .

Bidang	Opsi	Deskripsi
FeeType	`Authentication` , `Marketing` , `Service`, `Utility`, `Standard`	Bidang ini menampilkan jenis jenis percakapan yang digunakan, atau menentukan standar untuk biaya per pesan Kategori yang diprakarsai **`ConversationFee`** bisnis • `Marketing` — Digunakan untuk mencapai berbagai tujuan, mulai dari menghasil kan kesadaran hingga mendorong penjualan dan penargetan ulang pelanggan. Contohnya termasuk pengumuman produk, layanan, atau fitur baru, promosi/penawaran yang ditargetkan, dan pengingat pengabaian keranjang. • `Utility`— Digunakan untuk menindaklanjuti tindakan atau permintaa n pengguna. Contohnya termasuk konfirmasi keikutsertaan, manajemen pesanan/pengiriman (misalnya pembaruan pengiriman); pembaruan akun atau peringata n (misalnya pengingat pembayaran); atau survei umpan balik.

Bidang	Opsi	Deskripsi
		• `Authentication` — Digunakan untuk mengautentikasi pengguna dengan kode sandi satu kali, berpotensi pada beberapa langkah dalam proses login (misalnya verifikasi akun, pemulihan akun, dan tantangan integritas). • `Service`— Digunakan untuk menyelesaikan pertanyaan pelanggan. Kategori yang diprakarsai **`ConversationFee`** pengguna • `Service`— Digunakan untuk menyelesaikan pertanyaan pelanggan. **`MessageFee`** kategori • `Standard`— Per pesan yang dikirim atau diterima biaya.

Ketika Anda memulai percakapan dengan mengirim pesan template, Anda akan ditagih untuk satu `ConversationFee` dan satu. `MessageFee` Ini membuka jendela 24 jam di mana setiap pesan template yang Anda kirim ke pelanggan yang sama ditagih sebagai individu`MessageFee`. Selama jendela 24 jam, pesan template harus jenis yang sama atau percakapan baru dimulai.

Misalnya, jika Anda mengirim pesan template pemasaran ke pelanggan, Anda ditagih untuk `ConversationFee` dan`MessageFee`.

```
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
```

Jika pelanggan mengirimi Anda pesan dan Anda merespons, maka Anda ditagih untuk membuka `Service` percakapan dan pesan baru.

```
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
```

Contoh 1: Mengirim pesan template Pemasaran

Misalnya, jika Anda mengirim pesan template pemasaran ke pelanggan, Anda ditagih untuk satu WhatsApp `ConversationFee` dan satu AWS per `MessageFee` satu.

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

Contoh 2: Membuka percakapan Layanan

Biaya percakapan layanan berlaku ketika bisnis merespons pesan masuk pengguna yang berada di luar jendela percakapan 24 jam aktif yang diprakarsai oleh bisnis. Dalam skenario ini, Anda ditagih satu WhatsApp `ConversationFee` dan satu AWS `MessageFee` untuk setiap pesan masuk dan keluar.

```
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 Pesan Pengguna Akhir ISO Kode penagihan sosial dan pemetaan Biaya WhatsApp Percakapan

Negara yang didukung

Kode ISO negara dua digit	Negara Selatan	WhatsApp wilayah penagihan percakapan
AF	Afghanistan	Asia Pasifik
KAPAK	Kepulauan Cayman	Lainnya
AL	Albania	Sisa Eropa Tengah & Timur
DZ	Aljazair	Afrika Selatan
AS	Kepulauan Cayman	Lainnya
AD	Andorra	Lainnya
AO	Angola	Afrika Selatan
Al	Anguilla	Lainnya
AQ	Antartika	Lainnya
AG	Antigua dan Barbuda	Lainnya
AR	Argentina	Argentina
SAYA	Armenia	Sisa Eropa Tengah & Timur
STS	Aruba	Lainnya
AZ	Pulau Ascension	Lainnya
AZ	Australia	Asia Pasifik
DI	Austria	Sisa Eropa Barat
AZ	Azerbaijan	Sisa Eropa Tengah & Timur
BS	Bahama	Lainnya
BH	Bahrain	Timur Tengah

Kode ISO negara dua digit	Negara Selatan	WhatsApp wilayah penagihan percakapan
BD	Bangladesh	Asia Pasifik
BB	Barbados	Lainnya
OLEH	Belarus	Sisa Eropa Tengah & Timur
ADA	Belgium	Sisa Eropa Barat
BZ	Belize	Lainnya
BJ	Benin	Afrika Selatan
BM	Bermuda	Lainnya
BT	Bhutan	Lainnya
BO	Bolivia	Sisa Amerika Latin
BQ	Bonaire	Lainnya
AZ	Bosnia dan Herzegovina	Lainnya
BW	Botswana	Afrika Selatan
BV	Kepulauan Cayman	Lainnya
BR	Brazil	Brazil
IO	Wilayah Samudra Hindia Britania	Lainnya
.TV	Kepulauan Virgin	Lainnya
BN	Brunei	Lainnya
BG	Bulgaria	Sisa Eropa Tengah & Timur
BF	BurkinaFaso	Afrika Selatan

Kode ISO negara dua digit	Negara Selatan	WhatsApp wilayah penagihan percakapan
BI	Burundi	Afrika Selatan
KH	Kamboja	Asia Pasifik
CM	Kamerun	Afrika Selatan
CA	Kanada	Amerika Utara
CV	Tanjung Verde	Lainnya
KY	Kepulauan Cayman	Lainnya
LIH	Republik Afrika Tengah	Lainnya
TD	Chad	Afrika Selatan
CL	Chili	Chili
CN	Kepulauan Cayman	Asia Pasifik
CX	Pulau Natal	Lainnya
CC	Kepulauan Cocos (Keeling	Lainnya
CO	Kolombia	Kolombia
KM	Komoro	Lainnya
CG	Kongo	Lainnya
.FR	Kongo	Afrika Selatan
CK	Kepulauan Cook	Lainnya
CR	Kosta Rika	Sisa Amerika Latin
CI	Pantai Gading	Afrika Selatan
JAM	Croatia	Sisa Eropa Tengah & Timur

Kode ISO negara dua digit	Negara Selatan	WhatsApp wilayah penagihan percakapan
STS	Curacao	Lainnya
CY	Cyprus	Lainnya
CZ	Czech Republic	Sisa Eropa Tengah & Timur
DK	Denmark	Sisa Eropa Barat
DJ	Djibouti	Lainnya
.FR	Dominika	Lainnya
BERBUAT	Republik Dominika	Sisa Amerika Latin
EC	Ekuador	Sisa Amerika Latin
CONTOHNYA	Mesir	Mesir
SV	El Salvador	Sisa Amerika Latin
GQ	Guinea Khatulistiwa	Lainnya
ER	Eritrea	Afrika Selatan
EE	Estonia	Lainnya
ET	Etiopia	Afrika Selatan
FK	Kepulauan Falkland	Lainnya
FO	Kepulauan Faroe	Lainnya
FJ	Fiji	Lainnya
.FI	Finland	Sisa Eropa Barat
AZ	France	France
GF	Guyana Prancis	Lainnya

Kode ISO negara dua digit	Negara Selatan	WhatsApp wilayah penagihan percakapan
PF	Polinesia	Lainnya
TF	Wilayah Selatan Prancis	Lainnya
AZ	Gabon	Afrika Selatan
GM	Gambia	Afrika Selatan
GE	Georgia	Sisa Eropa Tengah & Timur
AZ	Germany	Germany
GH	Ghana	Afrika Selatan
GI	Gibraltar	Lainnya
GR	Greece	Sisa Eropa Tengah & Timur
GL	Greenland	Lainnya
GD	Grenada	Lainnya
GP	Guadeloupe	Lainnya
GU	Guam	Lainnya
GT	Guatemala	Sisa Amerika Latin
STS	Guernsey	Lainnya
GN	Guinea	Lainnya
GW	Guinea-Bissau	Afrika Selatan
GY	Guyana	Lainnya
HT	Haiti	Sisa Amerika Latin

Kode ISO negara dua digit	Negara Selatan	WhatsApp wilayah penagihan percakapan
HM	Heard dan McDonald Kepulauan	Lainnya
HN	Honduras	Sisa Amerika Latin
HK	Hong Kong	Asia Pasifik
HU	Hungary	Sisa Eropa Tengah & Timur
ADALAH	Islandia	Lainnya
DI DALAM	India	India
DI DALAM	India	India
ID	Indonesia	Indonesia
ID	Indonesia Internasional	Indonesia Internasional
IQ	Irak	Timur Tengah
YAKNI	Ireland	Sisa Eropa Barat
.IM	Pulau Man	Lainnya
IL	Israel	Israel
IA	Italy	Italy
JM	Jamaika	Sisa Amerika Latin
.FR	Jepang	Asia Pasifik
JE	Jersey	Lainnya
JO	Yordania	Timur Tengah
KZ	Kazakstan	Lainnya

Kode ISO negara dua digit	Negara Selatan	WhatsApp wilayah penagihan percakapan
KE	Kenya	Afrika Selatan
KI	Kiribati	Lainnya
XK	Kosovo	Lainnya
KW	Kuwait	Timur Tengah
KG	Kirgistan	Lainnya
LA	Laos PDR	Asia Pasifik
LV	Latvia	Sisa Eropa Tengah & Timur
LB	Libanon	Timur Tengah
LS	Lesotho	Afrika Selatan
LR	Liberia	Afrika Selatan
LY	Libya	Afrika Selatan
LI	Liechtenstein	Lainnya
LT	Lithuania	Sisa Eropa Tengah & Timur
LU	Luxembourg	Lainnya
MO	Makau	Lainnya
MK	Makedonia	Sisa Eropa Tengah & Timur
MG	Madagaskar	Afrika Selatan
MW	Malawi	Afrika Selatan
SAYA	Malaysia	Malaysia
MV	Maladewa	Lainnya

Kode ISO negara dua digit	Negara Selatan	WhatsApp wilayah penagihan percakapan
.TV	Mali	Afrika
MT	Malta	Lainnya
MH	Kepulauan Marshall	Lainnya
MQ	Martinik	Lainnya
TN.	Mauritania	Afrika
MU	Mauritius	Lainnya
.SHS	Mayotte	Lainnya
MX	Meksiko	Meksiko
.FR	Mikronesia	Lainnya
MD	Moldova	Sisa Eropa Tengah & Timur
MC	Monako	Lainnya
MN	Mongolia	Asia Pasifik
SAYA	Montenegro	Lainnya
MD	Montserrat	Lainnya
.TV	Maroko	Afrika
MZ	Mozambik	Afrika
MM	Myanmar	Lainnya
TA	Namibia	Afrika
NO	Nauru	Lainnya
NP	Nepal	Asia Pasifik

Kode ISO negara dua digit	Negara Selatan	WhatsApp wilayah penagihan percakapan
NL	Netherlands	Netherlands
NC	Kaledonia Baru	Lainnya
NZ	Selandia Baru	Asia Pasifik
NI	Nikaragua	Sisa Amerika Latin
NE	Niger	Afrika
NG	Nigeria	Nigeria
NU	Niue	Lainnya
AZ	Pulau Norfolk	Lainnya
MP	Kepulauan Mariana Utara	Lainnya
TIDAK	Norwegia	Sisa Eropa Barat
OM	Oman	Timur Tengah
PK	Pakistan	Pakistan
PW	Palau	Lainnya
PS	Wilayah Palestina	Lainnya
PA	Panama	Sisa Amerika Latin
PG	Papua Nugini	Asia Pasifik
PY	Paraguay	Sisa Amerika Latin
PE	Peru	Peru
PH	Filipina	Asia Pasifik
PN	Pitcairn	Lainnya

Kode ISO negara dua digit	Negara Selatan	WhatsApp wilayah penagihan percakapan
PL	Poland	Sisa Eropa Tengah & Timur
PT	Portugal	Sisa Eropa Barat
PR	Puerto Riko	Sisa Amerika Latin
QA	Qatar	Timur Tengah
KEMBALI	Reuni	Lainnya
RO	Romania	Sisa Eropa Tengah & Timur
RU	Federasi Rusia	Rusia
RW	Rwanda	Afrika
.SHS	Kepulauan Cayman	Lainnya
KN	Saint Kitts dan Nevis	Lainnya
LC	Saint Lucia	Lainnya
PM	Saint Pierre dan Miquelon	Lainnya
VC	Saint Vincent dan Grenadines	Lainnya
BL	Saint-Barthelemy	Lainnya
MF	Kepulauan Cayman	Lainnya
STS	Samoa	Lainnya
STS	San Marino	Lainnya
STS	Sao Tome dan Principe	Lainnya
.FI	Arab Saudi	Arab Saudi
SG-	Senegal	Afrika

Kode ISO negara dua digit	Negara Selatan	WhatsApp wilayah penagihan percakapan
RS	Serbia	Sisa Eropa Tengah & Timur
.TV	Seychelles	Lainnya
SL	Sierra Leone	Afrika
SG-	Singapura	Asia Pasifik
SX	Sint Maarten	Lainnya
SK	Slovakia	Sisa Eropa Tengah & Timur
SI	Slovenia	Sisa Eropa Tengah & Timur
SB	Kepulauan Solomon	Lainnya
BEGITU	Somalia	Afrika
/YTS	Afrika Selatan	Afrika Selatan
GS	Georgia Selatan dan Kepulauan Sandwich Selatan	Lainnya
KR	Korea Selatan	Lainnya
SS	Sudan Selatan	Afrika
ES	Spain	Spain
LK	Sri Lanka	Asia Pasifik
SR	Suriname	Lainnya
SJ	Kepulauan Svalbard dan Jan Mayen	Lainnya
SZ	Swaziland	Afrika
AZ	Sweden	Sisa Eropa Barat

Kode ISO negara dua digit	Negara Selatan	WhatsApp wilayah penagihan percakapan
CH	Swiss	Sisa Eropa Barat
TW	Taiwan	Asia Pasifik
TJ	Tajikistan	Asia Pasifik
TZ	Tanzania	Afrika
TH	Thailand	Asia Pasifik
TTS	Timor-Leste	Lainnya
TG	Togo	Afrika
TK	Tokelau	Lainnya
KE	Tonga	Lainnya
TT	Trinidad dan Tobago	Lainnya
TA	Trist dan Cunha	Lainnya
TN	Tunisia	Afrika
TR	Turki	Turki
TM	Turkmenistan	Asia Pasifik
TC	Kepulauan Turks dan Caicos	Lainnya
.TV	Tuvalu	Lainnya
UG	Uganda	Afrika
UA	Ukraina	Sisa Eropa Tengah & Timur
AZ	Uni Emirat Arab	Uni Emirat Arab
GB	Britania Raya	Britania Raya

Kode ISO negara dua digit	Negara Selatan	WhatsApp wilayah penagihan percakapan
AS	Amerika Serikat	Amerika Utara
UY	Uruguay	Sisa Amerika Latin
UM	Kepulauan Terluar Kecil AS	Lainnya
UZ	Uzbekistan	Asia Pasifik
VU	Vanuatu	Lainnya
VA	Negara Kota Vatikan	Lainnya
VE	Venezuela	Sisa Amerika Latin
VN	Vietnam	Asia Pasifik
VI	Kepulauan Virgin	Lainnya
WF	Kepulauan Wallis dan Futuna	Lainnya
EH	Sahara Barat	Lainnya
STS	Yaman	Timur Tengah
ZM	Zambia	Afrika
ZW	Zimbabwe	Lainnya

Pemantauan Pesan Pengguna AWS Akhir Sosial

Pemantauan adalah bagian penting dari pemeliharaan keandalan, ketersediaan, dan kinerja AWS End User Messaging Social dan AWS solusi lainnya. AWSmenyediakan alat pemantauan berikut untuk mengawasi AWS End User Messaging Social, melaporkan saat terjadi kesalahan, dan mengambil tindakan otomatis jika diperlukan:

- Amazon CloudWatch memantau AWS sumber daya Anda dan aplikasi yang Anda jalankan AWS di secara waktu nyata. Anda dapat mengumpulkan dan melacak metrik, membuat dasbor yang disesuaikan, dan mengatur alarm yang memberi tahu Anda atau mengambil tindakan saat metrik tertentu mencapai ambang batas yang ditentukan. Misalnya, Anda dapat membuat CloudWatch melacak CPU penggunaan atau metrik lain dari EC2 instans Amazon Anda dan secara otomatis meluncurkan instans baru ketika diperlukan. Untuk informasi selengkapnya, lihat Panduan CloudWatch Pengguna Amazon.
- Amazon CloudWatch Logs memungkinkan Anda memantau, menyimpan, dan mengakses file log dari EC2 instans Amazon, CloudTrail, dan sumber lainnya. CloudWatch Log dapat memantau informasi dalam file log dan memberi tahu Anda ketika ambang tertentu terpenuhi. Anda juga dapat mengarsipkan data log dalam penyimpanan yang sangat durabel. Untuk informasi selengkapnya, lihat Panduan Pengguna Amazon CloudWatch Logs.
- AWS CloudTrailmerekam API panggilan dan kejadian terkait yang dilakukan oleh atau atas nama AWS akun Anda dan mengirimkan file log ke bucket Amazon S3 yang Anda tentukan. Anda dapat mengidentifikasi pengguna dan akun mana yang memanggil AWS, alamat IP sumber yang melakukan panggilan, dan kapan panggilan tersebut terjadi. Untuk informasi selengkapnya, lihat Panduan Pengguna AWS CloudTrail.

Memantau Pesan Pengguna AWS Akhir Sosial dengan Amazon CloudWatch

Anda dapat memantau AWS End User Messaging Social CloudWatch, yang mengumpulkan data mentah dan memprosesnya menjadi metrik yang dapat dibaca dan hampir waktu nyata. Statistik ini disimpan untuk jangka waktu 15 bulan, sehingga Anda dapat mengakses informasi historis dan mendapatkan perspektif yang lebih baik tentang performa aplikasi atau layanan web Anda. Anda juga dapat mengatur alarm yang memperhatikan ambang batas tertentu dan mengirim notifikasi atau mengambil tindakan saat ambang batas tersebut terpenuhi. Untuk informasi selengkapnya, lihat Panduan CloudWatch Pengguna Amazon.

Untuk AWS End User Messaging Social, Anda mungkin ingin mengawasi`WhatsAppMessageFeeCount`, dan juga menonton `WhatsAppConversationFeeCount` dan memicu alarm ketika ambang batas pengeluaran telah tercapai.

Tabel berikut ini mencantumkan metrik dan dimensi yang diekspor AWS End User Messaging Social ke namespace. `AWS/SocialMessaging`

Metrik	Unit	Deskripsi
WhatsAppConversationFeeCount	Hitung	Hitungan biaya WhatsApp percakapan
WhatsAppMessageFeeCount	Hitung	Hitungan biaya WhatsApp pesan

Dimensi	Deskripsi
MessageFeeType	Jenis biaya yang valid adalah Layanan, Pemasaran, Utilitas, dan Otentikasi
DestinationCountryCode	ISOKode dua huruf untuk negara
WhatsAppPhoneNumberArn	Arn nomor telepon

Logging AWS End User Messaging API Panggilan sosial menggunakan AWS CloudTrail

AWS Panggilan yang direkam mencakup data yang direkam oleh pengguna yang menyediakan catatan yang AWS CloudTraildibuat oleh pengguna yang menyediakan catatan yang direkam oleh pengguna yang menyediakan catatan tindakan yang dilakukan oleh pengguna yang menyediakan catatan tindakan yang dilakukan oleh pengguna yang menyediakan catatan tindakan yang dilakukan oleh pengguna yang dibuat Layanan AWS oleh pengguna CloudTrail menangkap semua API panggilan untuk AWS End User Messaging Social sebagai acara. Panggilan yang direkam mencakup panggilan dari sumber daya di akun AWS AWS API Anda. AWS Menggunakan informasi yang dikumpulkan oleh Google CloudTrail, Anda dapat menentukan permintaan yang dibuat ke, alamat

IP asal permintaan tersebut dibuat ke AWS , alamat IP asal permintaan tersebut dibuat, siapa yang membuat permintaan tersebut dibuat, kapan permintaan dibuat, kapan permintaan dibuat ke, alamat IP asal permintaan tersebut dibuat, siapa yang membuat permintaan tersebut dibuat, siapa yang membuat permintaan tersebut dibuat, siapa yang membuat permintaan tersebut dibuat, siapa yang membuat permintaan tersebut dibuat ke

Setiap entri peristiwa atau log berisi informasi tentang siapa yang membuat permintaan tersebut. Informasi identitas membantu Anda menentukan berikut hal ini:

- Baik permintaan tersebut dibuat dengan kredensial pengguna root atau pengguna.
- Apakah permintaan dibuat atas nama pengguna Pusat IAM Identitas.
- Apakah permintaan tersebut dibuat dengan kredensial keamanan sementara untuk satu peran atau pengguna terfederasi.
- Apakah permintaan tersebut dibuat oleh Layanan AWS lain.

CloudTrail aktif di Anda Akun AWS ketika Anda membuat akun dan Anda secara otomatis memiliki akses ke riwayat CloudTrail Acara. Riwayat CloudTrail Acara menyediakan catatan yang dapat dilihat, dapat dicari, dapat diunduh, dan tidak dapat diubah dari 90 hari terakhir dari peristiwa manajemen yang direkam dalam file. Wilayah AWS Untuk informasi selengkapnya, lihat Bekerja dengan riwayat CloudTrail Acara di Panduan AWS CloudTrail Pengguna. Tidak ada CloudTrail biaya untuk melihat riwayat Acara.

Untuk informasi lebih lanjut tentang peristiwa di akun Akun AWS AWS Anda. CloudTrail

CloudTrail Jejak

Jejak memungkinkan CloudTrail untuk mengirim berkas log ke bucket Amazon S3. Semua jalur yang dibuat menggunakan AWS Management Console Multi-region. Anda dapat membuat jalur Single-region atau Multi-region dengan menggunakan. AWS CLI Membuat jejak Multi-wilayah disarankan karena Anda menangkap aktivitas Wilayah AWS di semua akun Anda. Jika Anda membuat jejak wilayah Tunggal, Anda hanya dapat melihat peristiwa yang dicatat di jejak. Wilayah AWS Untuk informasi selengkapnya tentang jejak, lihat Membuat jejak untuk Anda Akun AWS dan Membuat jejak untuk organisasi di Panduan AWS CloudTrail Pengguna.

Anda dapat mengirimkan satu salinan acara manajemen yang sedang berlangsung ke bucket Amazon S3 Anda tanpa biaya CloudTrail dengan membuat jejak, namun, ada biaya penyimpanan Amazon S3. Untuk informasi selengkapnya tentang CloudTrail harga, lihat AWS CloudTrail Harga. Untuk informasi tentang harga Amazon S3, lihat Harga Amazon S3.

CloudTrail Menyimpan data acara danau

CloudTrail Lake memungkinkan Anda menjalankan kueri SQL berbasis pada acara Anda. CloudTrail Lake mengonversi peristiwa yang ada dalam JSON format berbasis baris ke format Apache. ORC ORCadalah format penyimpanan kolumnar yang dioptimalkan untuk pengambilan data dengan cepat. Peristiwa digabungkan ke dalam penyimpanan data peristiwa, yang merupakan kumpulan peristiwa yang tidak dapat diubah berdasarkan kriteria yang Anda pilih dengan menerapkan pemilih acara tingkat lanjut. Penyeleksi yang Anda terapkan ke penyimpanan data acara mengontrol peristiwa mana yang bertahan dan tersedia untuk Anda kueri. Untuk informasi lebih lanjut tentang CloudTrail Danau, lihat Bekerja dengan AWS CloudTrail Danau di Panduan AWS CloudTrail Pengguna.

CloudTrail Penyimpanan data acara danau dan kueri menimbulkan biaya. Saat Anda membuat penyimpanan data acara, Anda memilih opsi harga yang ingin Anda gunakan untuk penyimpanan data acara. Opsi penetapan harga menentukan biaya untuk menelan dan menyimpan peristiwa, dan periode retensi default dan maksimum untuk penyimpanan data acara. Untuk informasi selengkapnya tentang CloudTrail harga, lihat AWS CloudTrail Harga.

AWS Pesan Pengguna Akhir Peristiwa data sosial di CloudTrail

Peristiwa data memberikan informasi tentang operasi sumber daya yang dilakukan pada atau di sumber daya (misalnya, membaca atau menulis ke objek Amazon S3). Ini juga dikenal sebagai operasi bidang data. Operasi ini sering kali merupakan peristiwa yang sering kali merupakan aktivitas yang dilakukan oleh pengguna. CloudTrail Nilai dari Riwayat CloudTrail peristiwa tidak merekam peristiwa data.

Biaya tambahan berlaku untuk peristiwa data. Untuk informasi selengkapnya tentang CloudTrail harga, lihat AWS CloudTrail Harga.

Anda dapat mencatat peristiwa data untuk jenis sumber daya Sosial Pesan Pengguna AWS Akhir menggunakan CloudTrail konsol AWS CLI, atau CloudTrail API operasi. Untuk informasi selengkapnya tentang cara mencatat peristiwa data, lihat Mencatat peristiwa data dengan AWS Management Console dan Logging peristiwa data dengan AWS Command Line Interface di Panduan AWS CloudTrail Pengguna.

Tabel berikut mencantumkan tipe sumber daya Sosial Pesan Pengguna AWS Akhir yang dapat Anda log peristiwa data. Kolom tipe peristiwa data (konsol) menunjukkan nilai yang akan dipilih dari daftar tipe peristiwa Data di CloudTrail konsol. Kolom nilai resources.type menunjukkan **`resources.type`** nilai, yang akan Anda tentukan saat mengonfigurasi penyeleksi acara lanjutan menggunakan or.

AWS CLI CloudTrail APIs CloudTrailKolom Data yang APIs dicatat ke menampilkan API panggilan yang dicatat CloudTrail untuk jenis sumber daya.

Jenis peristiwa data (konsol)	value	Data APIs masuk CloudTrail
ID Nomor Telepon Pesan Sosial	`AWS::SocialMessaging::PhoneNumberId`	• DeleteWhatsAppMessageMedia • GetWhatsAppMessageMedia • PostWhatsAppMessageMedia • SendWhatsAppMessage

Anda dapat mengonfigurasi pemilih acara lanjutan untuk memfilter pada `eventName`,`readOnly`, dan `resources.ARN` bidang untuk mencatat hanya peristiwa yang penting bagi Anda. Untuk informasi lebih lanjut tentang topik berikut, lihat topik berikut: AdvancedFieldSelectordalam AWS CloudTrail APIReferensi.

AWS End User Messaging Acara manajemen sosial di CloudTrail

Kegiatan manajemen memberikan informasi tentang operasi manajemen yang dilakukan berdasarkan sumber daya di akun AWS Anda Akun AWS. Ini juga dikenal sebagai operasi bidang data. Secara default, CloudTrail mencatat peristiwa manajemen.

AWS End User Messaging Social mencatat semua operasi bidang kontrol sosial Pesan Pengguna AWS Akhir sebagai peristiwa manajemen. Untuk daftar operasi bidang kontrol Sosial Pesan Pengguna AWS Akhir yang digunakan untuk log Sosial Pesan Pengguna AWS Akhir CloudTrail, lihat APIReferensi Sosial Pesan Pengguna AWS Akhir.

AWS Contoh acara Sosial Pesan Pengguna Akhir

Sebuah peristiwa mewakili satu permintaan dari sumber apa pun dan mencakup informasi tentang API operasi yang diminta, tanggal dan waktu tindakan yang diminta, tanggal dan waktu tindakan yang diminta, tanggal dan waktu tindakan yang diminta, tanggal dan waktu tindakan yang diminta, tanggal dan waktu tindakan yang diminta, tanggal dan waktu tindakan yang diminta, tanggal dan waktu operasi, parameter permintaan, CloudTrail Berkas log AWS bukan merupakan jejak tumpukan API terurut dari sumber daya di akun AWS Anda.

Contoh berikut menunjukkan objek CloudTrail acara tindakan penampil.

```
{
        "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"
        }
    }
```

Untuk informasi tentang konten CloudTrail rekaman, lihat konten CloudTrail rekaman di Panduan AWS CloudTrail Pengguna.

Praktik terbaik untuk AWS End User Messaging Sosial

Bagian ini menjelaskan beberapa praktik terbaik yang dapat membantu Anda meningkatkan keterlibatan pelanggan dan menghindari penangguhan akun. Namun, perhatikan bahwa bagian ini tidak berisi nasihat hukum. Selalu konsultasikan dengan pengacara untuk mendapatkan nasihat hukum.

Untuk daftar praktik WhatsApp terbaik terbaru, lihat Kebijakan Pesan WhatsApp Bisnis.

Topik

Up-to-date Pengguna root

Menjaga profil up-to-date WhatsApp Bisnis yang akurat yang mencakup informasi kontak dukungan pelanggan, seperti alamat email, alamat situs web, atau nomor telepon. Pastikan bahwa informasi yang diberikan adalah benar dan tidak salah menggambarkan atau menyamar sebagai bisnis lain.

Mendapatkan izin

Jangan pernah mengirim pesan ke penerima yang belum secara eksplisit meminta untuk menerima jenis pesan tertentu yang Anda rencanakan untuk dikirim. Kebencian kebijakan berikut:

- Proses keikutsertaan harus dengan jelas memberi tahu orang tersebut bahwa mereka setuju untuk menerima pesan atau panggilan dari bisnis Anda. WhatsApp Anda harus secara eksplisit menyatakan nama bisnis Anda.
- Anda bertanggung jawab penuh untuk menentukan metode untuk mendapatkan persetujuan keikutsertaan. Pastikan bahwa proses keikutsertaan mematuhi semua hukum yang berlaku yang mengatur komunikasi Anda. Berikan semua pemberitahuan yang diperlukan dan dapatkan semua izin yang diperlukan berdasarkan undang-undang yang relevan.

Untuk informasi selengkapnya tentang persyaratan WhatsApp Keikutsertaan, lihat Mendapatkan Keikutsertaan untuk WhatsApp

Jika penerima dapat mendaftar untuk menerima pesan Anda menggunakan formulir online, mencegah skrip otomatis membuat langganan tanpa sepengetahuan mereka. Juga batasi berapa kali pengguna dapat mengirimkan nomor telepon dalam satu sesi.

Hormati semua permintaan yang dibuat oleh seseorang, baik aktif atau tidak aktif WhatsApp, untuk memblokir, menghentikan, atau memilih keluar dari komunikasi, termasuk menghapus orang tersebut dari daftar kontak Anda.

Pertahankan catatan yang mencakup tanggal, waktu, dan sumber setiap permintaan dan konfirmasi keikutsertaan menerima pesan. Hal ini mungkin berguna jika operator atau badan pengawas memintanya, dan juga dapat membantu Anda melakukan audit rutin terhadap daftar pelanggan Anda.

Isi pesan.

Important

Bekerja dengan Meta/ WhatsApp

- Penggunaan Solusi WhatsApp Bisnis oleh Anda tunduk pada syarat dan ketentuan Ketentuan Layanan WhatsApp Bisnis, Ketentuan Solusi WhatsApp Bisnis, Kebijakan Pesan WhatsApp Bisnis, Pedoman Pesan, dan semua syarat, kebijakan, atau pedoman lain yang disertakan di dalamnya dengan referensi (karena masing-masing dapat diperbarui dari waktu ke waktu). WhatsApp
- Meta atau WhatsApp dapat sewaktu-waktu melarang penggunaan Solusi WhatsApp Bisnis oleh Anda.
- Sehubungan dengan penggunaan Solusi WhatsApp Bisnis oleh Anda, Anda tidak akan mengirimkan konten, informasi, atau data apa pun yang tunduk pada pengamanan atau pembatasan distribusi sesuai dengan hukum atau peraturan yang berlaku.

Jika Anda melanggar WhatsApp kebijakan, akun Anda dapat diblokir untuk mengirim pesan untuk jangka waktu tertentu, dikunci hingga Anda mengajukan banding, atau diblokir secara permanen. Meta akan memberi tahu Anda jika ada akun atau aset Anda yang melanggar kebijakan, melalui email dan Manajer WhatsApp Bisnis. Semua permohonan harus dilakukan ke Meta. Untuk melihat pelanggaran kebijakan atau mengajukan banding dengan Meta, lihat Melihat detail pelanggaran

kebijakan untuk akun WhatsApp Bisnis Anda di Pusat Bantuan Meta Business. Untuk daftar terbaru konten pesan terlarang, lihat Kebijakan Pesan WhatsApp Bisnis.

Berikut ini adalah kategori konten yang dilarang untuk semua jenis pesan secara global. Untuk memulai pesan berikut WhatsApp, ikuti panduan berikut:

Kategori	Contoh
Judi	• .loan • Undian • Aplikasi Tembakau
Peran terkait layanan yang bisa Anda gunakan untuk	• Logo Kredit • Pinjaman berbunga tinggi jangka pendek • Logo • Logo Kredit • Saldo Kredit • Tanda kutip saham • Pemberitahuan Aplikasi • Mata Uang Kripto
Pengampunan hutang	• Tagihan Terbatas • Gigi reduksi • Peran tertaut kredit
Get-rich-quick Kebijakan terkelola	• Work-from-home program • Peluang risiko-investasi • Skema pemasaran piramida atau multi-level
Zat ilegal	• Ganja/CBD
Phishing/smishing	• Upaya untuk membuat pengguna mengungkapkan informasi pribadi atau informasi login situs web.
S.H.A.F.T.	• Aplikasi

Kategori	Contoh
	• Simbol Kebencian • Alkohol • Senjata api • Amazon Records
Tagihan Terbatas	• Perusahaan yang membeli, menjual, atau berbagi informasi konsumen

Audit daftar pelanggan Anda

Jika Anda mengirim WhatsApp pesan berulang, audit daftar pelanggan Anda secara berkala. Mengaudit daftar pelanggan Anda membantu memastikan bahwa pelanggan yang menerima pesan Anda hanyalah mereka yang ingin menerimanya.

Saat Anda mengaudit daftar, kirim pesan kepada setiap pelanggan yang mengingatkan mereka bahwa mereka berlangganan, dan memberi mereka informasi tentang bagaimana cara berhenti berlangganan.

Sesuaikan pengiriman Anda berdasarkan keterlibatan

Prioritas pelanggan Anda dapat berubah seiring waktu. Jika pelanggan tidak lagi menganggap pesan Anda berguna, mereka mungkin memilih untuk tidak menerima pesan Anda sama sekali, atau bahkan melaporkan pesan Anda sebagai tidak diminta. Untuk alasan ini, penting untuk menyesuaikan praktik pengiriman berdasarkan keterlibatan pelanggan.

Untuk pelanggan yang jarang terlibat dengan pesan Anda, Anda harus menyesuaikan frekuensi pesan Anda. Misalnya, jika Anda mengirim pesan mingguan ke pelanggan yang terlibat, Anda dapat membuat rencana pengiriman bulanan terpisah untuk pelanggan yang kurang terlibat.

Lalu, hapus pelanggan yang benar-benar tidak terlibat dari daftar pelanggan Anda. Langkah ini mencegah pelanggan frustrasi terhadap pesan Anda. Ini juga menghemat pengeluaran Anda dan membantu melindungi reputasi Anda sebagai pengirim.

Kirim pada waktu yang tepat

Hanya kirim pesan selama jam kerja normal siang hari. Jika Anda mengirim pesan di waktu makan malam atau di tengah malam, ada kemungkinan bahwa pelanggan Anda akan berhenti berlangganan dari daftar Anda agar tidak terganggu. Anda mungkin ingin menghindari mengirim WhatsApp pesan ketika pelanggan Anda tidak dapat segera merespons pesan tersebut.

Keamanan di AWS End User Messaging Sosial

Keamanan cloud di AWS AWS merupakan prioritas tertinggi. Sebagai AWS pelanggan, Anda mendapatkan manfaat dari pusat data dan arsitektur jaringan yang dibangun untuk memenuhi persyaratan organisasi yang sangat mengutamakan keamanan.

Keamanan adalah tanggung jawab bersama antara AWS dan Anda. Model tanggung jawab bersama menjelaskan hal ini sebagai keamanan cloud dan keamanan dalam cloud:

- Keamanan cloud — AWS bertanggung jawab untuk melindungi infrastruktur yang menjalankan AWS layanan di AWS Cloud. AWS Amazon juga menyediakan layanan yang bisa Anda gunakan dengan aman. Auditor pihak ke tiga menguji dan memverifikasi efektivitas keamanan kami secara berkala sebagai bagian dari Program AWS Kepatuhan Program AWS . Untuk mempelajari tentang program kepatuhan yang berlaku untuk Pengguna AWS Akhir Pesan Sosial, lihat AWS Layanan dalam Cakupan melalui Program Kepatuhan AWS .
- Keamanan dalam cloud — Tanggung jawab Anda ditentukan oleh AWS layanan yang Anda gunakan. Anda juga bertanggung jawab atas faktor lain, yang mencakup sensitivitas data Anda, persyaratan perusahaan Anda, serta undang-undang dan peraturan yang berlaku.

Dokumentasi ini membantu Anda memahami cara menerapkan model tanggung jawab bersama saat menggunakan AWS End User Messaging Social. Topik berikut akan menunjukkan cara mengonfigurasi AWS End User Messaging Social untuk memenuhi tujuan keamanan dan kepatuhan Anda. Anda juga mempelajari cara menggunakan AWS layanan lain yang membantu Anda memantau dan mengamankan sumber daya Sosial Pesan Pengguna AWS Akhir.

Topik

Perlindungan data di AWS End User Messaging Social

Model tanggung jawab AWS bersama model berlaku untuk perlindungan data di AWS End User Messaging Social. Sebagaimana dijelaskan dalam model AWS ini, bertanggung jawab untuk melindungi infrastruktur global yang menjalankan semua AWS Cloud. Anda bertanggung jawab untuk mempertahankan kendali atas konten yang di-host pada infrastruktur ini. Anda juga bertanggung jawab atas tugas-tugas konfigurasi dan manajemen keamanan untuk Layanan AWS yang Anda gunakan. Untuk informasi selengkapnya tentang privasi data, lihat Privasi Data FAQ. Untuk informasi tentang perlindungan data di Eropa, lihat postingan blog Model Tanggung Jawab AWS Bersama dan postingan GDPR blog di Blog AWS Keamanan.

Untuk tujuan perlindungan data, kami merekomendasikan agar Anda melindungi Akun AWS kredensia dan menyiapkan pengguna individu dengan AWS IAM Identity Center atau AWS Identity and Access Management ()IAM. Dengan cara itu, setiap pengguna hanya diberi izin yang diperlukan untuk memenuhi tanggung jawab tugasnya. Kami juga menyarankan supaya Anda mengamankan data dengan cara-cara berikut:

- Gunakan autentikasi multifaktor (MFAMFA) pada setiap akun.
- GunakanSSL/TLSuntuk berkomunikasi dengan AWS sumber daya. Kami membutuhkan TLS 1.2 dan merekomendasikan TLS 1.3.
- Siapkan API akun pengguna dengan AWS CloudTrail Amazon Untuk informasi tentang penggunaan CloudTrail jejak untuk menangkap AWS aktivitas, lihat Bekerja dengan CloudTrail jejak di AWS CloudTrail Panduan Pengguna.
- Gunakan solusi AWS enkripsi, bersama dengan semua kontrol keamanan standar di dalamnya Layanan AWS.
- Gunakan layanan keamanan terkelola lanjut seperti Amazon Macie, yang membantu menemukan dan mengamankan data sensitif yang disimpan di Amazon S3.
- Jika Anda memerlukan FIPS 140-3 modul kriptografi yang divalidasi saat mengakses AWS melalui antarmuka baris perintah atau, gunakan titik akhir. API FIPS Untuk informasi selengkapnya tentang FIPS titik akhir yang tersedia, lihat Standar Pemrosesan Informasi Federal (FIPS) 140-3.

Kami sangat merekomendasikan agar Anda tidak pernah memasukkan informasi identifikasi yang sensitif, seperti nomor rekening pelanggan Anda, ke dalam tanda atau bidang isian bebas seperti bidang Nama. Ini termasuk saat Anda bekerja dengan AWS End User Messaging Social atau lainnya Layanan AWS menggunakan konsol,API, AWS CLI, atau AWS SDKs. Data apa pun yang Anda masukkan ke dalam tanda atau bidang isian bebas yang digunakan untuk nama dapat

digunakan untuk log penagihan atau log diagnostik. Jika Anda memberikan URL ke server eksternal, kami sangat menyarankan agar Anda tidak menyertakan informasi kredenial di dalam URL untuk memvalidasi permintaan Anda ke server itu.

> **Important**
>
> WhatsApp menggunakan protokol Signal untuk komunikasi yang aman. Namun, karena AWS End User Messaging Social adalah pihak ketiga, WhatsApp tidak menganggap pesan ini end-to-end dienkripsi. Untuk informasi selengkapnya tentang perlindungan WhatsApp data, lihat whitepaper Ikhtisar Privasi & Keamanan Data dan WhatsApp Enkripsi.

Enkripsi data

AWS Pesan Pengguna Akhir Data sosial dienkripsi di transit dan saat tidak digunakan di dalam batas. AWS Ketika Anda mengirimkan data ke AWS End User Messaging Social, itu mengenkripsi data saat diterima dan menyimpannya. Saat Anda mengambil data dari AWS End User Messaging Social, data akan ditransmisikan kepada Anda dengan menggunakan protokol keamanan saat ini.

Enkripsi diam

AWS End User Messaging Social mengenkripsi semua data yang disimpan untuk Anda dalam batas. AWS Ini termasuk data konfigurasi, data registrasi, dan data apa pun yang Anda tambahkan ke AWS End User Messaging Social. Untuk mengenkripsi data Anda, AWS End User Messaging Social menggunakan kunci internal AWS Key Management Service (AWS KMS) yang dimiliki dan dikelola oleh layanan atas nama Anda. Untuk mengetahui informasi selengkapnya tentang AWS KMS, lihat AWS Key Management Service Panduan Developer .

Enkripsi bergerak

AWS End User Messaging Penggunaan sosial HTTPS dan Transport Layer Security (TLS) 1.2 untuk berkomunikasi dengan klien, aplikasi, dan Meta Anda. Untuk berkomunikasi dengan AWS layanan lain, AWS End User Messaging Social menggunakan HTTPS dan TLS 1.2. Selain itu, ketika Anda membuat dan mengelola AWS SMS sumber daya dengan menggunakan konsol AWS SDK, atau AWS Command Line Interface, semua komunikasi diamankan menggunakan HTTPS dan TLS 1.2.

Manajemen kunci

Untuk mengenkripsi data Anda, AWS End User Messaging Social menggunakan AWS KMS kunci internal yang dimiliki dan dikelola oleh layanan atas nama Anda. Anda bisa mengunduh pesan. Anda tidak dapat menyediakan dan menggunakan kunci Anda sendiri AWS KMS atau lainnya untuk mengenkripsi data yang Anda simpan di Sosial Pesan Pengguna AWS Akhir.

Privasi lalu lintas antar jaringan

Privasi lalu lintas Internetwork mengacu pada mengamankan koneksi dan lalu lintas antara AWS End User Messaging Social dan klien dan aplikasi lokal Anda, dan antara AWS End User Messaging Social dan AWS sumber daya lainnya dalam hal yang sama. Wilayah AWS Fitur dan praktik berikut dapat membantu Anda mengamankan privasi lalu lintas internetwork untuk AWS End User Messaging Social.

Lalu lintas antara AWS SMS layanan dan klien lokal

Untuk membuat koneksi pribadi antara AWS End User Messaging Social dan klien serta aplikasi di jaringan on-premises, Anda dapat menggunakannya AWS Direct Connect. Ini memungkinkan Anda untuk menghubungkan jaringan Anda ke suatu AWS Direct Connect lokasi dengan menggunakan kabel Ethernet serat optik standar. Salah satu ujung kabel terhubung ke router Anda. Ujung lainnya terhubung ke AWS Direct Connect router. Untuk informasi selengkapnya, lihat Apa itu AWS Direct Connect? dalam AWS Direct Connect Panduan Pengguna.

Untuk membantu mengamankan akses ke AWS End User Messaging Social melalui publikasiAPIs, kami sarankan Anda mematuhi persyaratan Sosial Pesan Pengguna AWS Akhir untuk API panggilan. AWS End User Messaging Social mengharuskan klien untuk menggunakan Transport Layer Security (TLS) 1.2 atau lebih baru. Klien juga harus mendukung cipher suites dengan Perfect Forward Secrecy (PFS), seperti Ephemeral Diffie-Hellman () atau Elliptic Curve Diffie-Hellman Ephemeral (). DHE ECDHE Sebagian besar sistem modern seperti Java 7 dan versi lebih baru mendukung mode-mode ini.

Selain itu, permintaan harus ditandatangani menggunakan access key ID dan secret access key yang terkait dengan prinsipal AWS Identity and Access Management (IAM) untuk AWS akun Anda. Atau, Anda dapat menggunakan AWS Security Token Service(AWS STS) untuk membuat kredensi keamanan sementara untuk menandatangani permintaan.

Identity and access management untuk AWS akun pengguna dengan Amazon Control

AWS Identity and Access Management (IAM) adalah sebuah Layanan AWS yang membantu administrator dalam mengendalikan akses ke AWS sumber daya dengan aman. IAMadministrator mengontrol siapa yang dapat terautentikasi (masuk) dan berwenang (memiliki izin) untuk menggunakan sumber daya Sosial Pesan Pengguna AWS Akhir. IAMadalah Layanan AWS yang dapat Anda gunakan tanpa biaya tambahan.

Topik

Audiens

Cara menggunakan AWS Identity and Access Management (IAM) berbeda, tergantung pada pekerjaan yang Anda lakukan di AWS End User Messaging Social.

Pengguna layanan — Jika Anda menggunakan layanan Sosial Pesan Pengguna AWS Akhir untuk melakukan tugas Anda, administrator Anda akan memberikan kredenial dan izin yang dibutuhkan. Saat Anda menggunakan lebih banyak fitur Sosial Pesan Pengguna AWS Akhir untuk melakukan pekerjaan, Anda mungkin memerlukan izin tambahan. Memahami cara akses dikelola dapat membantu Anda meminta izin yang tepat dari administrator Anda. Jika Anda tidak dapat mengakses fitur di AWS End User Messaging Social, lihatPemecahan Masalah Pesan Pengguna AWS Akhir Identitas sosial dan akses.

Administrator layanan — Jika Anda bertanggung jawab atas sumber daya Sosial Pesan Pengguna AWS Akhir di perusahaan Anda, Anda mungkin memiliki akses penuh ke AWS End User Messaging Sosial. Anda bertanggung jawab untuk menentukan fitur dan sumber daya AWS End User Messaging mana yang dapat diakses pengguna layanan Anda. Anda kemudian harus mengirimkan permintaan ke IAM administrator untuk mengubah izin pengguna layanan. Tinjau informasi di halaman ini untuk

memahami konsep dasarIAM. Untuk mempelajari selengkapnya tentang cara perusahaan Anda dapat menggunakan IAM dengan AWS End User Messaging Social, lihatCara Kerja AWS End User Messaging Social IAM.

IAMadministrator — Jika Anda adalah IAM administrator, Anda mungkin ingin mempelajari lebih detail tentang cara Anda menulis kebijakan untuk mengelola akses ke Sosial Pesan Pengguna AWS Akhir. Untuk melihat contoh Pesan Pengguna AWS Akhir Kebijakan berbasis identitas sosial yang dapat Anda gunakan, lihat. IAM Contoh kebijakan berbasis identitas untuk AWS End User Messaging Social

Mengautentikasi dengan identitas

Autentikasi adalah cara Anda masuk ke AWS menggunakan kredenal identitas Anda. Anda harus diautentikasi (masuk ke AWS) sebagai Pengguna root akun AWS, sebagai IAM pengguna, atau dengan mengambil peranIAM.

Anda dapat masuk AWS sebagai identitas federasi dengan menggunakan kredensil yang disediakan melalui sumber identitas. AWS IAM Identity Center Pengguna (Pusat IAM Identitas), otentikasi sign-on tunggal perusahaan Anda, dan kredensi Google atau Facebook Anda adalah contoh identitas federasi. Saat Anda masuk sebagai identitas federasi, administrator Anda sebelumnya menyiapkan federasi identitas menggunakan IAM peran. Ketika Anda mengakses AWS dengan menggunakan federasi, Anda secara tidak langsung mengambil peran.

Bergantung pada jenis pengguna Anda, Anda dapat masuk ke AWS Management Console atau portal AWS akses. Untuk informasi selengkapnya tentang masuk AWS, lihat Cara masuk ke Panduan AWS Sign-In Pengguna Anda Akun AWS.

Jika Anda mengakses AWS secara terprogram, AWS sediakan kit pengembangan perangkat lunak (SDK) dan antarmuka baris perintah (CLI) untuk menandatangani permintaan Anda secara kriptografis dengan menggunakan kredensil Anda. Jika Anda tidak menggunakan AWS alat, Anda harus menandatangani permintaan tersebut sendiri. Untuk informasi selengkapnya tentang menggunakan metode yang disarankan untuk menandatangani permintaan sendiri, lihat Menandatangani AWS API permintaan di Panduan IAM Pengguna.

Apa pun metode autentikasi yang digunakan, Anda mungkin diminta untuk menyediakan informasi keamanan tambahan. Misalnya, AWS menyarankan agar Anda menggunakan autentikasi multi-faktor (MFA) untuk meningkatkan keamanan akun Anda. Untuk mempelajari lebih lanjut, lihat Autentikasi multi-faktor di Panduan AWS IAM Identity Center Pengguna dan Menggunakan autentikasi multi-faktor (MFA) AWS di Panduan Pengguna. IAM

Akun AWS pengguna root

Saat Anda membuat akun Akun AWS, Anda memulai dengan satu identitas masuk yang memiliki akses penuh ke semua sumber daya Layanan AWS dan sumber daya dalam akun tersebut. Identitas ini disebut pengguna Akun AWS root dan diakses dengan cara masuk menggunakan alamat email dan kata sandi yang Anda gunakan untuk membuat akun. Kami sangat menyarankan agar Anda tidak menggunakan pengguna root untuk tugas sehari-hari. Lindungi kredensial pengguna root Anda dan gunakan kredensial tersebut untuk melakukan tugas yang hanya dapat dilakukan pengguna root. Untuk daftar lengkap tugas yang mengharuskan Anda masuk sebagai pengguna utama, lihat Tugas yang memerlukan kredenal pengguna root di IAMPanduan Pengguna.

Identitas gabungan

Sebagai praktik terbaik, mewajibkan pengguna manusia, termasuk pengguna yang memerlukan akses administrator, untuk menggunakan federasi dengan penyedia identitas untuk mengakses Layanan AWS dengan menggunakan kredensi sementara.

Identitas federasi adalah pengguna dari direktori pengguna perusahaan Anda, penyedia identitas web, direktori Pusat Identitas AWS Directory Service, atau pengguna mana pun yang mengakses Layanan AWS dengan menggunakan kredensil yang disediakan melalui sumber identitas. Ketika identitas federasi mengakses Akun AWS, mereka mengambil peran, dan peran memberikan kredensi sementara.

Untuk manajemen akses terpusat, kami sarankan Anda menggunakan AWS IAM Identity Center. Anda dapat membuat pengguna dan grup di Pusat IAM Identitas, atau Anda dapat menghubungkan dan menyinkronkan ke sekumpulan pengguna dan grup di sumber identitas Anda sendiri untuk digunakan di semua aplikasi Akun AWS dan aplikasi Anda. Untuk informasi tentang Pusat IAM Identitas, lihat Apa itu Pusat IAM Identitas? dalam AWS IAM Identity Center User Guide.

Pengguna dan grup IAM

IAMPengguna adalah identitas dalam akun Anda Akun AWS yang memiliki izin khusus untuk satu orang atau aplikasi. Jika memungkinkan, sebaiknya Anda mengandalkan kredensi sementara alih-alih membuat IAM pengguna yang memiliki kredensi jangka panjang seperti kata sandi dan kunci akses. Namun, jika Anda memiliki kasus penggunaan khusus yang memerlukan kredensil jangka panjang dengan IAM pengguna, kami sarankan Anda memutar kunci akses. Untuk informasi selengkapnya, lihat Memutar kunci akses secara teratur untuk kasus penggunaan yang memerlukan kredensi jangka panjang di IAMPanduan Pengguna.

IAMGrup adalah identitas yang menentukan kumpulan IAM pengguna. Anda tidak dapat masuk sebagai grup. Anda dapat menggunakan grup untuk menentukan izin bagi beberapa pengguna sekaligus. Grup mempermudah manajemen izin untuk sejumlah besar pengguna sekaligus. Misalnya, Anda dapat memiliki grup dengan nama IAMAdminsdan memberikan izin kepada grup tersebut untuk mengelola sumber dayaIAM.

Pengguna berbeda dari peran. Pengguna secara unik terkait dengan satu orang atau aplikasi, tetapi peran dimaksudkan untuk dapat digunakan oleh siapa pun yang membutuhkannya. Pengguna memiliki kredensial jangka panjang permanen, tetapi peran memberikan kredensial sementara. Untuk mempelajari lebih lanjut, lihat Kapan membuat IAM pengguna (bukan peran) di Panduan IAM Pengguna.

IAMperan

IAMPeran adalah identitas dalam diri Anda Akun AWS yang memiliki izin khusus. Peran ini mirip dengan IAM pengguna, tetapi tidak terkait dengan orang tertentu. Anda dapat menjalankan IAM peran sementara di AWS Management Console dengan beralih peran. Anda dapat mengambil peran dengan memanggil AWS CLI atau AWS API operasi atau dengan menggunakan kustomURL. Untuk informasi selengkapnya tentang metode penggunaan peran, lihat Metode untuk mengambil peran dalam Panduan IAM Pengguna.

IAMperan dengan kredenal sementara berguna dalam situasi berikut:

- Akses pengguna terfederasi – Untuk menetapkan izin ke identitas terfederasi, Anda membuat peran dan menentukan izin untuk peran tersebut. Ketika identitas terfederasi mengautentikasi, identitas tersebut terhubung dengan peran dan diberi izin yang ditentukan oleh peran. Untuk informasi tentang peran untuk federasi, lihat Membuat peran untuk Penyedia Identitas pihak ketiga di Panduan IAM Pengguna. Jika Anda menggunakan Pusat IAM Identitas, Anda mengonfigurasi set izin. Untuk mengontrol apa yang dapat diakses identitas Anda setelah diautentikasi, Pusat IAM Identitas mengkorelasikan izin yang disetel ke peran. IAM Untuk informasi tentang set izin, lihat Set izin dalam Panduan Pengguna AWS IAM Identity Center .
- Izin IAM pengguna sementara — IAM Pengguna atau peran dapat mengambil IAM peran sementara untuk mengambil izin yang berbeda bagi tugas tertentu.
- Akses lintas akun — Anda dapat menggunakan IAM peran untuk mengizinkan seseorang (prinsipal terpercaya) di akun yang berbeda untuk mengakses sumber daya dalam akun Anda. Peran adalah cara utama untuk memberikan akses lintas akun. Namun, pada beberapa Layanan AWS, Anda dapat melampirkan kebijakan langsung ke sumber daya (alih-alih menggunakan peran sebagai

proksi). Untuk mempelajari perbedaan kebijakan berbasis peran dan sumber daya untuk akses lintas akun, lihat Akses sumber daya lintas akun di IAM Panduan Pengguna. IAM

- Akses lintas layanan — Beberapa Layanan AWS menggunakan fitur di lainnya Layanan AWS. Misalnya, saat Anda melakukan panggilan dalam suatu layanan, merupakan hal yang biasa bagi layanan tersebut untuk menjalankan aplikasi di Amazon EC2 atau menyimpan objek di Amazon S3. Sebuah layanan mungkin melakukannya menggunakan izin prinsipal yang memanggil, menggunakan peran layanan, atau peran terkait layanan.
  - Sesi akses teruskan (FAS) — Saat Anda menggunakan IAM pengguna atau peran untuk melakukan tindakan di AWS, Anda dianggap sebagai prinsipal. Ketika Anda menggunakan beberapa layanan, Anda mungkin melakukan sebuah tindakan yang kemudian menginisiasi tindakan lain di layanan yang berbeda. FASmenggunakan izin dari pemanggilan utama Layanan AWS, dikombinasikan dengan permintaan Layanan AWS untuk membuat permintaan ke layanan hilir. FASPermintaan hanya dibuat ketika layanan menerima permintaan yang memerlukan interaksi dengan orang lain Layanan AWS atau sumber daya untuk menyelesaikannya. Dalam hal ini, Anda harus memiliki izin untuk melakukan kedua tindakan tersebut. Untuk detail kebijakan saat membuat FAS permintaan, lihat Meneruskan sesi akses.
  - Peran layanan — Peran layanan adalah IAMperan yang diambil oleh layanan untuk melakukan tindakan atas nama Anda. IAMAdministrator dapat membuat, memodifikasi, dan menghapus peran layanan dari dalamIAM. Untuk informasi selengkapnya, lihat Membuat peran untuk mendelegasikan izin ke Layanan AWS dalam IAMPanduan Pengguna.
  - Peran tertaut-layanan — Peran tertaut-layanan adalah jenis peran layanan yang tertaut dengan peran layanan. Layanan AWS Layanan tersebut dapat menjalankan peran untuk melakukan tindakan atas nama Anda. Peran terkait layanan muncul di Anda Akun AWS dan dimiliki oleh layanan tersebut. IAMAdministrator dapat melihat, tetapi tidak dapat mengedit izin untuk peran yang ditautkan dengan layanan.
- Aplikasi yang berjalan di Amazon EC2 — Anda dapat menggunakan IAM peran untuk mengelola kredenal sementara untuk aplikasi yang berjalan pada EC2 instance dan membuat AWS CLI atau AWS API meminta. Ini lebih disukai daripada menyimpan kunci akses di dalam EC2 instans. Untuk menetapkan AWS peran ke EC2 instans dan membuatnya tersedia untuk semua aplikasinya, Anda membuat profil instans yang terlampir ke instans. Profil instans berisi peran dan memungkinkan program yang berjalan di EC2 instans untuk mendapatkan kredensi sementara. Untuk informasi selengkapnya, lihat Menggunakan IAM peran untuk memberikan izin ke aplikasi yang berjalan di EC2 instans Amazon di IAMPanduan Pengguna.

Untuk mempelajari apakah akan menggunakan IAM peran atau IAM pengguna, lihat Kapan membuat IAM peran (bukan pengguna) di Panduan IAM Pengguna.

Mengelola akses menggunakan kebijakan

Anda mengontrol akses di AWS dengan membuat kebijakan dan melampirkannya ke AWS identitas atau sumber daya. Kebijakan adalah objek di, AWS yang saat terkait dengan identitas atau sumber daya, akan menentukan izinnya. AWS mengevaluasi kebijakan ini saat penanggung jawab (pengguna, pengguna akar, atau sesi peran) mengajukan permintaan. Izin dalam kebijakan menentukan apakah permintaan diizinkan atau ditolak. Sebagian besar kebijakan disimpan dalam AWS JSON kebijakan. Untuk informasi selengkapnya tentang struktur dan isi dokumen JSON kebijakan, lihat Ringkasan JSON kebijakan di Panduan IAM Pengguna.

Administrator dapat menggunakan AWS JSON kebijakan untuk menentukan siapa yang memiliki akses ke hal apa. Yaitu, principal dapat melakukan tindakan pada suatu sumber daya, dan dalam suatu syarat.

Secara default, pengguna dan peran tidak memiliki izin. Untuk memberikan izin kepada para pengguna untuk melakukan tindakan di sumber daya yang mereka perlukan, IAM administrator dapat membuat IAM kebijakan. Administrator kemudian dapat menambahkan IAM kebijakan ke peran, dan pengguna dapat mengambil peran.

IAMKebijakan mendefinisikan izin untuk tindakan terlepas dari metode yang Anda gunakan untuk melakukan operasi. Misalnya, anggaplah Anda memiliki kebijakan yang mengizinkan tindakan `iam:GetRole`. Pengguna dengan kebijakan itu bisa mendapatkan informasi peran dari AWS Management Console, AWS CLI, atau AWS API.

Kebijakan berbasis identitas

Kebijakan berbasis identitas adalah dokumen kebijakan JSON izin yang dapat Anda lampirkan ke suatu identitas, seperti pengguna, grup IAM pengguna, atau peran. Kebijakan ini mengontrol jenis tindakan yang dapat dilakukan oleh pengguna dan peran, di sumber daya mana, dan berdasarkan kondisi seperti apa. Untuk mempelajari cara membuat kebijakan berbasis identitas, lihat Membuat IAM kebijakan di Panduan Pengguna. IAM

Kebijakan berbasis identitas dapat dikategorikan lebih lanjut sebagai kebijakan inline atau kebijakan yang dikelola. Kebijakan inline disematkan langsung ke satu pengguna, grup, atau peran. Kebijakan terkelola adalah kebijakan mandiri yang dapat diterapkan ke beberapa pengguna, grup, dan peran dalam. Akun AWS Kebijakan yang dikelola meliputi kebijakan yang AWS dikelola meliputi kebijakan yang dikelola dan kebijakan yang dikelola meliputi kebijakan yang dikelola meliputi kebijakan yang

dikelola Untuk mempelajari cara memilih antara kebijakan terkelola atau kebijakan inline, lihat Memilih antara kebijakan terkelola dan kebijakan inline di IAMPanduan Pengguna.

Kebijakan berbasis sumber daya

Kebijakan berbasis sumber daya adalah dokumen JSON kebijakan yang Anda lampirkan ke sumber daya. Contoh kebijakan berbasis sumber daya adalah kebijakan kepercayaan IAM peran dan kebijakan bucket Amazon S3. Dalam layanan yang mendukung kebijakan berbasis sumber daya, administrator layanan dapat menggunakannya untuk mengontrol akses ke sumber daya tertentu. Untuk sumber daya tempat kebijakan dilampirkan, kebijakan menentukan tindakan apa yang dapat dilakukan oleh prinsipal tertentu pada sumber daya tersebut dan dalam kondisi apa. Anda harus menentukan prinsipal dalam kebijakan berbasis sumber daya. Prinsipal dapat mencakup akun, pengguna, peran, pengguna federasi, atau. Layanan AWS

Kebijakan berbasis sumber daya merupakan kebijakan inline yang terletak di layanan tersebut. Anda tidak dapat menggunakan kebijakan yang AWS dikelola dari IAM kebijakan berbasis sumber daya.

Daftar kontrol akses (ACLACLs)

Access control list (ACLs) mengontrol pelaku utama mana (anggota akun, pengguna, atau peran) yang memiliki izin untuk mengakses sumber daya. ACLsserupa dengan kebijakan berbasis sumber daya, meskipun tidak menggunakan format dokumen kebijakan. JSON

Amazon S3, AWS WAF, dan Amazon VPC adalah contoh layanan yang mendukung. ACLs Untuk mempelajari selengkapnyaACLs, lihat Gambaran umum daftar kontrol akses (ACL) dalam Panduan Developer Amazon Simple Storage Service.

Jenis-jenis kebijakan lain

AWS Hal ini terkait kebijakan tambahan yang kurang lazim. Jenis-jenis kebijakan ini dapat mengatur izin maksimum yang diberikan kepada Anda oleh jenis kebijakan yang lebih umum.

- Batas izin — Batas izin adalah fitur lanjutan di mana Anda mengatur izin maksimum yang dapat diberikan oleh kebijakan berbasis identitas ke entitas (pengguna atau peran). IAM IAM Anda dapat menetapkan batasan izin untuk suatu entitas. Izin yang dihasilkan adalah perpotongan antara kebijakan berbasis identitas milik entitas dan batasan izinnya. Kebijakan berbasis sumber daya yang menentukan pengguna atau peran dalam bidang `Principal` tidak dibatasi oleh batasan izin. Penolakan eksplisit dalam salah satu kebijakan ini akan menggantikan pemberian izin. Untuk informasi selengkapnya tentang batas izin, lihat Batas izin untuk IAM entitas di IAMPanduan Pengguna.

- Kebijakan kontrol layanan (SCPs) — SCPs adalah JSON kebijakan yang menentukan izin maksimum untuk sebuah organisasi atau unit organisasional (OU) di AWS Organizations. AWS Organizations adalah layanan untuk mengelompokkan dan secara terpusat mengelola beberapa Akun AWS yang dimiliki bisnis Anda. Jika Anda mengaktifkan semua fitur dalam suatu organization, maka Anda dapat menerapkan kebijakan kontrol layanan (SCPs) ke setiap atau semua akun Anda. SCPMembatasi izin untuk entitas di akun anggota, termasuk masing-masing Pengguna root akun AWS. Untuk informasi selengkapnya tentang Organizations danSCPs, lihat Kebijakan kontrol layanan di Panduan AWS Organizations Pengguna.
- Kebijakan sesi – Kebijakan sesi adalah kebijakan lanjutan yang Anda berikan sebagai parameter ketika Anda membuat sesi sementara secara programatis untuk peran atau pengguna terfederasi. Izin sesi yang dihasilkan adalah perpotongan antara kebijakan berbasis identitas pengguna atau peran dan kebijakan sesi. Izin juga bisa datang dari kebijakan berbasis sumber daya. Penolakan secara tegas dalam salah satu kebijakan ini membatalkan izin. Untuk informasi selengkapnya, lihat Kebijakan sesi di Panduan IAM Pengguna.

Berbagai jenis kebijakan

Ketika beberapa jenis kebijakan berlaku pada suatu permintaan, izin yang dihasilkan lebih rumit untuk dipahami. Untuk mempelajari cara AWS menentukan apakah akan mengizinkan permintaan jika beberapa jenis kebijakan dilibatkan, lihat Logika evaluasi kebijakan di Panduan IAM Pengguna.

Cara Kerja AWS End User Messaging Social IAM

Sebelum Anda gunakan IAM untuk mengelola akses ke AWS End User Messaging Social, Anda harus memahami IAM fitur apa yang tersedia untuk digunakan dengan AWS End User Messaging Social.

IAMfitur yang dapat Anda gunakan dengan AWS End User Messaging Social

IAMfitur	AWS Dukungan Sosial End User Messaging
Kebijakan berbasis identitas	Ya
Kebijakan berbasis sumber daya	Tidak
Tindakan kebijakan	Ya

IAMfitur	AWS Dukungan Sosial End User Messaging
Sumber daya kebijakan	Ya
Kunci kondisi kebijakan	Ya
ACLs	Tidak
ABAC(tag dalam kebijakan)	Parsial
Kredensial sementara	Ya
Izin prinsipal	Ya
Peran layanan	Ya
Peran terkait layanan	Ya

Untuk mendapatkan tampilan tingkat tinggi tentang cara Layanan AWS End User Messaging Sosial dan AWS layanan lainnya bekerja dengan sebagian besar IAM fitur, lihat AWS Layanan yang bekerja IAM di Panduan IAM Pengguna.

Kebijakan berbasis identitas AWS untuk

Kebijakan berbasis identitas untuk

Kebijakan berbasis identitas adalah dokumen kebijakan JSON izin yang dapat Anda lampirkan ke suatu identitas, seperti pengguna, grup IAM pengguna, atau peran. Kebijakan ini mengontrol jenis tindakan yang dapat dilakukan oleh pengguna dan peran, di sumber daya mana, dan berdasarkan kondisi seperti apa. Untuk mempelajari cara membuat kebijakan berbasis identitas, lihat Membuat IAM kebijakan di Panduan Pengguna. IAM

Dengan kebijakan IAM berbasis identitas, Anda dapat menentukan tindakan dan sumber daya yang diizinkan atau ditolak, serta kondisi diperbolehkan atau ditolak. Anda tidak dapat menentukan secara spesifik prinsipal dalam sebuah kebijakan berbasis identitas karena prinsipal berlaku bagi pengguna atau peran yang melekat kepadanya. Untuk mempelajari semua elemen yang dapat Anda gunakan dalam JSON kebijakan, lihat referensi elemen IAM JSON kebijakan di Panduan IAM Pengguna.

Contoh kebijakan berbasis identitas untuk AWS End User Messaging Social

Untuk melihat contoh kebijakan berbasis identitas Pengguna AWS Akhir, lihat. Contoh kebijakan berbasis identitas untuk AWS End User Messaging Social

Kebijakan berbasis sumber daya dalam AWS Amplient

Mendukung kebijakan berbasis sumber daya dalam kebijakan berbasis sumber daya

Kebijakan berbasis sumber daya adalah dokumen JSON kebijakan yang Anda lampirkan ke sumber daya. Contoh kebijakan berbasis sumber daya adalah kebijakan kepercayaan IAM peran dan kebijakan bucket Amazon S3. Dalam layanan yang mendukung kebijakan berbasis sumber daya, administrator layanan dapat menggunakannya untuk mengontrol akses ke sumber daya tertentu. Untuk sumber daya tempat kebijakan dilampirkan, kebijakan menentukan tindakan apa yang dapat dilakukan oleh prinsipal tertentu pada sumber daya tersebut dan dalam kondisi apa. Anda harus menentukan prinsipal dalam kebijakan berbasis sumber daya. Prinsipal dapat mencakup akun, pengguna, peran, pengguna federasi, atau. Layanan AWS

Untuk mengaktifkan akses lintas akun, Anda dapat menentukan seluruh akun atau IAM entitas di akun lain sebagai penanggung jawab kebijakan berbasis sumber daya. Menambahkan prinsipal akun silang ke kebijakan berbasis sumber daya hanya setengah dari membangun hubungan kepercayaan. Ketika prinsipal dan sumber daya berbeda Akun AWS, IAM administrator di akun tepercaya juga harus memberikan izin entitas prinsipal (pengguna atau peran) untuk mengakses sumber daya tersebut. Mereka memberikan izin dengan melampirkan kebijakan berbasis identitas kepada entitas. Namun, jika kebijakan berbasis sumber daya memberikan akses ke prinsipal dalam akun yang sama, tidak diperlukan kebijakan berbasis identitas tambahan. Untuk informasi selengkapnya, lihat Akses sumber daya lintas akun IAM di Panduan IAM Pengguna.

Tindakan kebijakan untuk AWS End User Messaging Sosial

Mendukung tindakan kebijakan: Ya

Administrator dapat menggunakan AWS JSON kebijakan untuk menentukan siapa yang memiliki akses ke hal apa. Yaitu, principal dapat melakukan tindakan pada suatu sumber daya, dan dalam suatu syarat.

`Action`Elemen JSON kebijakan menjelaskan tindakan yang dapat Anda gunakan untuk mengizinkan atau menolak akses dalam kebijakan. Tindakan kebijakan biasanya memiliki nama yang sama dengan AWS API operasi terkait. Ada beberapa pengecualian, seperti tindakan khusus izin yang tidak memiliki operasi yang sesuai. API Ada juga beberapa operasi yang memerlukan beberapa tindakan dalam suatu kebijakan. Tindakan tambahan ini disebut tindakan dependen.

Menyertakan tindakan dalam kebijakan untuk memberikan izin untuk melakukan operasi terkait.

Untuk melihat daftar tindakan Sosial Pesan Pengguna AWS Akhir, lihat Tindakan yang Ditentukan oleh Sosial Pesan Pengguna AWS Akhir di Referensi Otorisasi Layanan.

Tindakan kebijakan di AWS End User Messaging Social menggunakan prefiks berikut sebelum tindakan:

```
social-messaging
```

Untuk menetapkan secara spesifik beberapa tindakan dalam satu pernyataan, pisahkan tindakan tersebut dengan koma.

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

Untuk melihat contoh kebijakan berbasis identitas Pengguna AWS Akhir, lihat. Contoh kebijakan berbasis identitas untuk AWS End User Messaging Social

Sumber daya kebijakan untuk AWS End User Messaging Social

Mendukung sumber daya kebijakan: Ya

Administrator dapat menggunakan AWS JSON kebijakan untuk menentukan siapa yang memiliki akses ke hal apa. Yaitu, principal dapat melakukan tindakan pada suatu sumber daya, dan dalam suatu syarat.

Elemen `Resource` JSON kebijakan menentukan objek di mana tindakan berlaku. Pernyataan harus menyertakan elemen `Resource` atau `NotResource`. Sebagai praktik terbaik, tentukan sumber daya menggunakan Amazon Resource Name (ARN). Anda dapat melakukan ini untuk tindakan yang mendukung jenis sumber daya tertentu, yang dikenal sebagai izin tingkat sumber daya.

Untuk tindakan yang tidak mendukung izin di tingkat sumber daya, misalnya operasi pencantuman, gunakan wildcard (*) untuk menunjukkan bahwa pernyataan tersebut berlaku untuk semua sumber daya.

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

Untuk melihat daftar jenis sumber daya Sosial Pesan Pengguna AWS Akhir dan jenis sumber daya SosialARNs, lihat Sumber Daya yang Ditentukan oleh Sosial Pesan Pengguna AWS Akhir di Referensi Otorisasi Layanan. Untuk mempelajari tindakan mana yang dapat menentukan setiap sumber daya, lihat Tindakan yang Ditentukan oleh Sosial Pesan Pengguna AWS Akhir. ARN

Untuk melihat contoh kebijakan berbasis identitas Pengguna AWS Akhir, lihat. Contoh kebijakan berbasis identitas untuk AWS End User Messaging Social

Kebijakan berbasis identitas untuk pengguna layanan AWS untuk pengguna layanan untuk layanan

Mendukung kunci kondisi kebijakan khusus layanan: Ya

Administrator dapat menggunakan AWS JSON kebijakan untuk menentukan siapa yang memiliki akses ke hal apa. Yaitu, di mana utama dapat melakukan tindakan pada sumber daya, dan dalam kondisi apa.

Elemen `Condition` (atau blok `Condition`) akan memungkinkan Anda menentukan kondisi yang menjadi dasar suatu pernyataan berlaku. Elemen `Condition` bersifat opsional. Anda dapat membuat ekspresi bersyarat yang menggunakan operator kondisi, misalnya sama dengan atau kurang dari, untuk mencocokkan kondisi dalam kebijakan dengan nilai-nilai yang diminta.

Jika Anda menentukan beberapa elemen `Condition` dalam sebuah pernyataan, atau beberapa kunci dalam elemen `Condition` tunggal, maka AWS akan mengevaluasinya menggunakan operasi `AND` logis. Jika Anda menetapkan beberapa nilai untuk kunci ketentuan tunggal, AWS mengevaluasi ketentuan tersebut menggunakan `OR` operasi logis. Semua kondisi harus dipenuhi sebelum izin pernyataan diberikan.

Anda juga dapat menggunakan variabel placeholder saat menentukan kondisi. Misalnya, Anda dapat memberikan izin IAM pengguna untuk mengakses sumber daya hanya jika ditandai dengan nama IAM pengguna mereka. Untuk informasi selengkapnya, lihat elemen IAM kebijakan: variabel dan tag di Panduan IAM Pengguna.

AWS mendukung kunci ketentuan global dan kunci ketentuan khusus layanan. Untuk melihat semua kunci kondisi AWS global, lihat kunci konteks kondisi AWS global dalam Panduan IAM Pengguna.

Untuk melihat daftar kunci kondisi Sosial Pesan Pengguna AWS Akhir, lihat Kunci Kondisi untuk Sosial Pesan Pengguna AWS Akhir di Referensi Otorisasi Layanan. Untuk mempelajari tindakan dan sumber daya mana yang dapat Anda gunakan kunci ketentuan, lihat Tindakan yang Ditentukan oleh AWS End User Messaging Social.

Untuk melihat contoh kebijakan berbasis identitas Pengguna AWS Akhir, lihat. Contoh kebijakan berbasis identitas untuk AWS End User Messaging Social

ACLsdi AWS End User Messaging Sosial

MendukungACLs: Tidak

Access control list (ACLs) mengontrol pelaku utama mana (anggota akun, pengguna, atau peran) yang memiliki izin untuk mengakses sumber daya. ACLsserupa dengan kebijakan berbasis sumber daya, meskipun tidak menggunakan format dokumen kebijakan. JSON

ABACdengan AWS End User Messaging Sosial

Mendukung ABAC (tag dalam kebijakan): Sebagian

Kontrol akses berbasis atribut (ABAC) adalah strategi otorisasi yang mendefinisikan izin berdasarkan atribut. Di AWS, atribut ini disebut tanda. Anda dapat melampirkan tag ke IAM entitas (pengguna atau peran) dan ke banyak AWS sumber daya. Menandai entitas dan sumber daya adalah langkah pertama dari. ABAC Kemudian Anda merancang ABAC kebijakan untuk mengizinkan operasi ketika tag penanggung jawab cocok dengan tag pada sumber daya yang mereka coba akses.

ABACsangat membantu di lingkungan yang berkembang dengan cepat dan membantu dalam situasi ketika manajemen kebijakan menjadi rumit.

Untuk mengendalikan akses berdasarkan tag, berikan informasi tentang tag di elemen kondisi dari kebijakan menggunakan kunci kondisi `aws:ResourceTag/`*`key-name`*, `aws:RequestTag/`*`key-name`*, atau `aws:TagKeys`.

Jika sebuah layanan mendukung ketiga kunci kondisi untuk setiap jenis sumber daya, nilainya adalah Ya untuk layanan tersebut. Jika suatu layanan mendukung ketiga kunci kondisi untuk hanya beberapa jenis sumber daya, nilainya adalah Parsial.

Untuk informasi lebih lanjut tentangABAC, lihat Apa ituABAC? dalam IAMUser Guide. Untuk melihat tutorial dengan langkah-langkah penyiapanABAC, lihat Menggunakan kontrol akses berbasis atribut (ABAC) di IAMPanduan Pengguna.

Menggunakan kredensi sementara dengan Amazon AWS EKS

Mendukung kredensi sementara: Ya

Beberapa Layanan AWS tidak berfungsi saat Anda masuk menggunakan kredenal sementara. Untuk informasi tambahan, termasuk yang Layanan AWS bekerja dengan kredenial sementara, lihat Layanan AWS yang bekerja dengan itu IAM di IAMPanduan Pengguna.

Anda menggunakan kredensi sementara jika Anda masuk ke AWS Management Console menggunakan metode apa pun kecuali nama pengguna dan kata sandi. Misalnya, ketika Anda mengakses AWS menggunakan link sign-on (SSO) tunggal perusahaan Anda, proses tersebut secara otomatis membuat kredensi sementara. Anda juga akan secara otomatis membuat kredensial sementara ketika Anda masuk ke konsol sebagai seorang pengguna lalu beralih peran. Untuk informasi selengkapnya tentang peralihan peran, lihat Beralih ke peran (konsol) di Panduan IAM Pengguna.

Anda dapat secara manual membuat kredensil sementara menggunakan atau. AWS CLI AWS API Anda kemudian dapat menggunakan kredensil sementara tersebut untuk mengakses. AWS AWS merekomendasikan agar Anda secara dinamis menghasilkan kredensi sementara alih-alih menggunakan kunci akses jangka panjang. Untuk informasi selengkapnya, lihat Kredensi keamanan sementara di. IAM

Izin prinsipal lintas layanan untuk AWS End User Messaging Social

Mendukung sesi akses maju (FAS): Ya

Saat Anda menggunakan IAM pengguna atau peran untuk melakukan tindakan di AWS, Anda dianggap sebagai pelaku utama. Ketika Anda menggunakan beberapa layanan, Anda mungkin melakukan sebuah tindakan yang kemudian menginisiasi tindakan lain di layanan yang berbeda. FASmenggunakan izin dari pemanggilan utama Layanan AWS, dikombinasikan dengan permintaan Layanan AWS untuk membuat permintaan ke layanan hilir. FASPermintaan hanya dibuat ketika layanan menerima permintaan yang memerlukan interaksi dengan orang lain Layanan AWS atau sumber daya untuk menyelesaikannya. Dalam hal ini, Anda harus memiliki izin untuk melakukan kedua tindakan tersebut. Untuk detail kebijakan saat membuat FAS permintaan, lihat Meneruskan sesi akses.

Peran layanan untuk AWS End User Messaging Social

Mendukung peran layanan: Ya

Peran layanan adalah IAMperan yang diasumsikan oleh layanan untuk melakukan tindakan atas nama Anda. IAMAdministrator dapat membuat, memodifikasi, dan menghapus peran layanan dari dalamIAM. Untuk informasi selengkapnya, lihat Membuat peran untuk mendelegasikan izin ke Layanan AWS dalam IAMPanduan Pengguna.

> **Warning**
>
> Mengubah izin untuk peran layanan dapat merusak fungsionalitas Sosial Pesan Pengguna AWS Akhir. Edit peran layanan hanya jika AWS End User Messaging Social memberikan panduan untuk melakukannya.

Peran terkait AWS layanan untuk

mendukung peran yang terkait layanan untuk

Peran yang ditautkan dengan layanan adalah jenis peran layanan yang tertaut dengan peran terkait layanan adalah jenis peran layanan yang tertaut dengan. Layanan AWS Layanan tersebut dapat menjalankan peran untuk melakukan tindakan atas nama Anda. Peran terkait layanan muncul di Anda Akun AWS dan dimiliki oleh layanan tersebut. IAMAdministrator dapat melihat, tetapi tidak dapat mengedit izin untuk peran yang ditautkan dengan layanan.

Untuk informasi selengkapnya tentang cara membuat atau mengelola peran yang tertaut dengan layanan, lihat AWS layanan yang bekerja dengannya. IAM Cari layanan dalam tabel yang memiliki `Yes` di kolom Peran terkait layanan. Pilih tautan Ya untuk melihat dokumentasi peran terkait layanan untuk layanan tersebut.

Contoh kebijakan berbasis identitas untuk AWS End User Messaging Social

Secara default, pengguna dan peran tidak memiliki izin untuk membuat atau memodifikasi sumber daya Sosial Pesan Pengguna AWS Akhir. Mereka juga tidak dapat melakukan tugas dengan menggunakan AWS Management Console, AWS Command Line Interface (AWS CLI), atau AWS API. Untuk memberikan izin kepada para pengguna untuk melakukan tindakan di sumber daya yang mereka perlukan, IAM administrator dapat membuat IAM kebijakan. Administrator kemudian dapat menambahkan IAM kebijakan ke peran, dan pengguna dapat mengambil peran.

Untuk mempelajari cara membuat kebijakan IAM berbasis identitas menggunakan contoh dokumen kebijakan ini, lihat Membuat JSON IAM kebijakan di Panduan Pengguna. IAM

Untuk detail tentang tindakan dan jenis sumber daya yang ditentukan oleh Sosial Pesan Pengguna AWS Akhir, termasuk format ARNs untuk setiap jenis sumber daya, lihat Tindakan, Sumber Daya, dan Kunci Kondisi untuk Sosial Pesan Pengguna AWS Akhir dalam Referensi Otorisasi Layanan.

Topik

- Praktik terbaik kebijakan
- Menggunakan konsol Sosial Pesan Pengguna AWS Akhir
- Mengizinkan pengguna melihat izin mereka sendiri

Praktik terbaik kebijakan

Kebijakan berbasis identitas menentukan apakah seseorang dapat membuat, mengakses, atau menghapus sumber daya Sosial Pesan Pengguna AWS Akhir di akun Anda. Tindakan ini membuat Akun AWS Anda dikenai biaya. Ketika Anda membuat atau mengedit kebijakan berbasis identitas, ikuti panduan dan rekomendasi ini:

- Mulailah dengan kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit — Untuk mulai memberikan izin kepada pengguna dan beban kerja Anda, gunakan kebijakan AWS terkelola yang memberikan izin untuk banyak kasus penggunaan umum. Mereka tersedia di Anda Akun AWS. Kami menyarankan Anda mengurangi izin lebih lanjut dengan menentukan kebijakan yang dikelola AWS pelanggan yang khusus untuk kasus penggunaan Anda. Untuk informasi selengkapnya, lihat kebijakan AWSAWS terkelola atau kebijakan terkelola untuk fungsi pekerjaan di Panduan IAM Pengguna.
- Menerapkan izin hak akses terkecil — Saat Anda menetapkan izin dengan IAM kebijakan, berikan hanya izin yang diperlukan untuk melaksanakan tugas. Anda melakukannya dengan mendefinisikan tindakan yang dapat diambil pada sumber daya tertentu dalam kondisi tertentu, yang juga dikenal sebagai izin dengan hak akses paling rendah. Untuk informasi selengkapnya tentang penggunaan IAM untuk menerapkan izin, lihat Kebijakan dan izin IAM di IAM Panduan Pengguna.
- Gunakan ketentuan dalam IAM kebijakan untuk membatasi akses lebih lanjut — Anda dapat menambahkan kondisi ke kebijakan Anda untuk membatasi akses ke tindakan dan sumber daya. Misalnya, Anda dapat menulis kondisi kebijakan untuk menentukan bahwa semua permintaan harus dikirim menggunakanSSL. Anda juga dapat menggunakan ketentuan untuk memberikan akses ke tindakan layanan jika digunakan melalui yang spesifik Layanan AWS, seperti AWS CloudFormation. Untuk informasi selengkapnya, lihat elemen IAM JSON kebijakan: Kondisi dalam Panduan IAM Pengguna.

- Gunakan IAM Access Analyzer untuk memvalidasi IAM kebijakan Anda guna memastikan izin yang aman dan fungsional — IAM Access Analyzer memvalidasi kebijakan baru dan yang sudah ada sehingga kebijakan mematuhi bahasa IAM kebijakan () JSON dan praktik terbaik. IAM IAMAccess Analyzer menyediakan lebih dari 100 pemeriksaan kebijakan dan rekomendasi yang dapat ditindaklanjuti untuk membantu Anda membuat kebijakan yang aman dan fungsional. Untuk informasi selengkapnya, lihat Validasi kebijakan IAM Access Analyzer di IAMPanduan Pengguna.
- Memerlukan otentikasi multi-faktor (MFA) - Jika Anda memiliki skenario yang mengharuskan IAM pengguna atau pengguna root di Anda Akun AWS, aktifkan MFA untuk keamanan tambahan. Untuk meminta MFA kapan API operasi dipanggil, tambahkan MFA kondisi ke kebijakan Anda. Untuk informasi selengkapnya, lihat Mengonfigurasi API akses MFA yang dilindungi di IAMPanduan Pengguna.

Untuk informasi selengkapnya tentang praktik terbaik diIAM, lihat Praktik terbaik keamanan IAM di Panduan IAM Pengguna.

Menggunakan konsol Sosial Pesan Pengguna AWS Akhir

Untuk mengakses konsol Sosial Perpesanan Pengguna AWS Akhir, Anda harus memiliki rangkaian izin minimum. Izin ini harus memperbolehkan Anda untuk membuat daftar dan melihat detail tentang sumber daya Sosial Pesan Pengguna AWS Akhir di akun Anda Akun AWS. Jika Anda membuat kebijakan berbasis identitas yang lebih ketat daripada izin minimum yang diperlukan, konsol tidak akan berfungsi sebagaimana mestinya untuk entitas (pengguna atau peran) dengan kebijakan tersebut.

Anda tidak perlu mengizinkan konsol minimum untuk pengguna yang melakukan panggilan hanya ke AWS CLI atau. AWS API Alih-alih, izinkan akses hanya ke tindakan yang sesuai dengan API operasi yang mereka coba lakukan.

Untuk memastikan bahwa pengguna dan peran masih dapat menggunakan konsol Sosial Pesan Pengguna AWS Akhir, lampirkan juga kebijakan Sosial `ConsoleAccess` atau `ReadOnly` AWS terkelola Pengguna AWS Akhir ke entitas. Untuk informasi selengkapnya, lihat Menambahkan izin ke pengguna di Panduan IAM Pengguna.

Mengizinkan pengguna melihat izin mereka sendiri

Contoh ini menunjukkan bagaimana Anda dapat membuat kebijakan yang memungkinkan IAM pengguna melihat kebijakan inline dan kebijakan terkelola yang terlampir pada identitas pengguna

mereka. Kebijakan ini mencakup izin untuk menyelesaikan tindakan ini di konsol atau secara terprogram menggunakan atau. AWS CLI 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 kebijakan terkelola untuk AWS End User Messaging Social

Untuk menambahkan izin ke pengguna, grup, dan peran, lebih mudah menggunakan kebijakan AWS terkelola daripada membuat kebijakan sendiri. Butuh waktu dan keahlian untuk membuat kebijakan yang dikelola IAM pelanggan yang hanya menyediakan izin yang dibutuhkan oleh tim Anda. Untuk memulai dengan cepat, Anda dapat menggunakan kebijakan AWS terkelola. Kebijakan ini mencakup kasus penggunaan umum dan tersedia di Akun AWS Anda. Untuk informasi selengkapnya tentang kebijakan AWS AWS terkelola, lihat kebijakan terkelola di Panduan IAM Pengguna.

AWS layanan memelihara dan memperbarui kebijakan AWS terkelola. Anda tidak dapat mengubah izin dalam kebijakan AWS terkelola. Layanan terkadang menambahkan izin tambahan ke kebijakan yang dikelola AWS untuk mendukung fitur-fitur baru. Jenis pembaruan ini akan memengaruhi semua identitas (pengguna, grup, dan peran) di mana kebijakan tersebut dilampirkan. Layanan kemungkinan besar akan memperbarui kebijakan yang dikelola AWS saat ada fitur baru yang diluncurkan atau saat ada operasi baru yang tersedia. Layanan tidak menghapus izin dari kebijakan yang AWS dikelola oleh, sehingga pembaruan kebijakan tidak akan merusak izin yang ada.

Selain itu, AWS mendukung kebijakan yang dikelola untuk fungsi tugas yang mencakup beberapa layanan. Misalnya, kebijakan ReadOnlyAccess AWS terkelola menyediakan akses hanya baca ke semua AWS layanan dan sumber daya. Saat layanan meluncurkan fitur baru, AWS tambahkan izin hanya baca untuk operasi dan sumber daya baru. Untuk daftar dan deskripsi kebijakan fungsi tugas, lihat Kebijakan AWS terkelola untuk fungsi tugas tugas tugas dalam Panduan IAM Pengguna.

AWS End User Messaging Pembaruan sosial ke kebijakan AWS terkelola

Lihat detail tentang pembaruan kebijakan AWS terkelola untuk AWS End User Messaging Social sejak layanan ini mulai melacak perubahan-perubahan tersebut. Untuk peringatan otomatis tentang perubahan pada halaman ini, berlangganan RSS umpan pada halaman riwayat Dokumen Sosial Pesan Pengguna AWS Akhir.

Perubahan	Deskripsi	Tanggal
AWS End User Messaging Sosial mulai melacak perubahan	AWS End User Messaging Sosial mulai melacak perubahan untuk kebijakan AWS terkelola.	26 September 2017

Pemecahan Masalah Pesan Pengguna AWS Akhir Identitas sosial dan akses

Gunakan informasi berikut untuk membantu Anda mendiagnosis dan memperbaiki masalah umum yang mungkin Anda temukan saat bekerja dengan AWS End User Messaging Social danIAM.

Topik

Saya tidak diotorisasi untuk melakukan tindakan di AWS End User Messaging Social

Jika Anda menerima pesan kesalahan bahwa Anda tidak memiliki otorisasi untuk melakukan tindakan, kebijakan Anda harus diperbarui agar Anda dapat melakukan tindakan tersebut.

Contoh kesalahan berikut terjadi ketika `mateojackson` IAM pengguna mencoba menggunakan konsol untuk melihat detail tentang *`my-example-widget`* sumber daya fiktif, tetapi tidak memiliki izin fiktif`social-messaging:`*`GetWidget`*.

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

Dalam hal ini, kebijakan untuk pengguna `mateojackson` harus diperbarui untuk mengizinkan akses ke sumber daya *`my-example-widget`* dengan menggunakan tindakan `social-messaging:`*`GetWidget`*.

Jika Anda tidak menggunakan alat bantu AWS Anda. Administrator Anda adalah orang yang memberi Anda kredensial masuk.

Saya tidak berwenang untuk melakukan iam:PassRole PassRole

Jika Anda menerima kesalahan bahwa Anda tidak terotorisasi untuk melakukan `iam:PassRole` tindakan, kebijakan Anda harus diperbarui agar Anda dapat meneruskan peran ke Sosial Pesan Pengguna AWS Akhir.

Beberapa Layanan AWS memungkinkan Anda untuk memberikan peran yang sudah ada ke layanan tersebut alih-alih membuat peran layanan baru atau peran tertaut-layanan. Untuk melakukannya, Anda harus memiliki izin untuk meneruskan peran ke layanan.

Contoh kesalahan berikut terjadi saat IAM pengguna yang bernama `marymajor` mencoba menggunakan konsol tersebut untuk melakukan tindakan di Sosial Pesan Pengguna AWS Akhir. Namun, tindakan tersebut memerlukan layanan untuk mendapatkan izin yang diberikan oleh peran layanan. Mary tidak memiliki izin untuk meneruskan peran tersebut pada layanan.

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

Dalam kasus ini, kebijakan Mary harus diperbarui agar dia mendapatkan izin untuk melakukan tindakan `iam:PassRole` tersebut.

Jika Anda tidak menggunakan alat bantu AWS Anda. Administrator Anda adalah orang yang memberi Anda kredensial masuk.

Saya ingin mengizinkan orang di luar saya Akun AWS untuk mengakses sumber daya Sosial Pesan Pengguna AWS Akhir saya

Anda dapat membuat peran yang dapat digunakan pengguna di akun lain atau orang-orang di luar organisasi Anda untuk mengakses sumber daya Anda. Anda dapat menentukan siapa saja yang dipercaya untuk mengambil peran tersebut. Untuk layanan yang mendukung kebijakan berbasis sumber daya atau daftar kontrol akses (ACLs), Anda dapat menggunakan kebijakan tersebut untuk memberi orang akses ke sumber daya Anda.

Untuk mempelajari selengkapnya, periksa referensi berikut:

- Untuk mempelajari apakah AWS End User Messaging Social mendukung fitur-fitur ini, lihatCara Kerja AWS End User Messaging Social IAM.
- Untuk mempelajari cara memberikan akses ke sumber daya Anda di seluruh Akun AWS yang Anda miliki, lihat Menyediakan akses ke IAM pengguna di lain Akun AWS yang Anda miliki di Panduan IAM Pengguna.
- Untuk mempelajari cara memberikan akses ke sumber daya Anda ke pihak ketiga Akun AWS, lihat Menyediakan akses ke yang Akun AWS dimiliki oleh pihak ke tiga dalam Panduan IAM Pengguna.
- Untuk mempelajari cara memberikan akses melalui federasi identitas, lihat Menyediakan akses ke pengguna yang diautentikasi secara eksternal (federasi identitas) di Panduan Pengguna. IAM

- Untuk mempelajari perbedaan antara menggunakan kebijakan berbasis peran dan sumber daya untuk akses lintas akun, lihat Akses sumber daya lintas akun di IAM Panduan Pengguna. IAM

Validasi kepatuhan untuk AWS End User Messaging Social

Untuk mempelajari apakah program kepatuhan tertentu, lihat dalam Cakupan melalui Program Kepatuhan Layanan AWS dalam Cakupan melalui Program Layanan AWS Kepatuhan dan memilih program kepatuhan yang Anda minati. Layanan AWS Untuk informasi umum, lihat Program AWS Kepatuhan Program AWS .

Anda bisa mengunduh laporan audit pihak ketiga menggunakan AWS Artifact. Untuk informasi selengkapnya, lihat Mengunduh Laporan AWS Artifact .

Tanggung jawab kepatuhan Anda saat menggunakan Layanan AWS ditentukan oleh sensitivitas data Anda, tujuan kepatuhan perusahaan Anda, serta undang-undang dan peraturan yang berlaku. AWS Gunakan sumber daya berikut untuk membantu kepatuhan berikut untuk membantu kepatuhan terhadap daftar pelanggan Anda.

- Panduan Quick Start Keamanan dan Kepatuhan — Panduan deployment ini membahas pertimbangan arsitektur dan memberikan langkah-langkah untuk men-deploy lingkungan dasar di AWS yang menjadi fokus keamanan dan kepatuhan.
- Arsitek untuk HIPAA Keamanan dan Kepatuhan di Amazon Web Services — Laporan resmi ini menjelaskan cara perusahaan dapat menggunakan AWS untuk membuat HIPAA aplikasi yang memenuhi syarat.

> **Note**
>
> Tidak semua Layanan AWS HIPAA memenuhi syarat. Untuk informasi selengkapnya, lihat Referensi Layanan yang HIPAA Memenuhi Syarat.

- AWS Sumber Daya AWS — Kumpulan buku kerja dan panduan ini mungkin berlaku untuk industri dan lokasi Anda.
- AWS Panduan Kepatuhan Pelanggan - Memahami model tanggung jawab bersama melalui lensa kepatuhan. Panduan ini merangkum praktik terbaik untuk mengamankan Layanan AWS dan memetakan panduan untuk kontrol keamanan di berbagai kerangka kerja (termasuk Institut Standar dan Teknologi Nasional (NIST), Dewan Standar Keamanan Industri Kartu Pembayaran (PCI), dan Organisasi Internasional untuk Standardisasi ()). ISO

- Mengevaluasi Sumber Daya dengan Aturan di Panduan AWS Config Developer — AWS Config Layanan menilai seberapa baik konfigurasi sumber daya Anda sesuai dengan praktik internal, pedoman industri, dan peraturan.
- AWS Security Hub— Ini Layanan AWS memberikan pandangan komprehensif tentang status keamanan Anda di AWS. Security Hub menggunakan kontrol keamanan untuk sumber daya AWS Anda serta untuk memeriksa kepatuhan Anda terhadap standar industri keamanan dan praktik terbaik. Untuk daftar layanan dan kontrol yang didukung, lihat Referensi kontrol Security Hub.
- Amazon GuardDuty — Ini Layanan AWS mendeteksi potensi ancaman terhadap beban kerja Akun AWS, kontainer, dan data Anda dengan memantau lingkungan Anda untuk aktivitas yang mencurigakan dan berbahaya. GuardDuty dapat membantu Anda mengatasi berbagai persyaratan kepatuhan, seperti PCIDSS, dengan memenuhi persyaratan deteksi intrusi yang diamanatkan oleh kerangka kerja kepatuhan tertentu.
- AWS Audit Manager— Ini akan Layanan AWS membantu Anda dalam meng-audit AWS Anda secara berkelanjutan untuk menyederhanakan cara Anda mengelola risiko dan kepatuhan terhadap peraturan dan standar industri.

Ketahanan dalam Pesan Pengguna AWS Akhir Sosial

Infrastruktur AWS global dibangun di sekitar Wilayah AWS dan Availability Zones. Wilayah AWS menyediakan beberapa Availability Zone yang terpisah secara fisik dan terisolasi, yang terhubung dengan jaringan berlatensi rendah, throughput yang tinggi, dan sangat redundan. Dengan Zona Ketersediaan, Anda dapat merancang serta mengoperasikan aplikasi dan basis data yang secara otomatis melakukan fail over di antara zona tanpa gangguan. Zona Ketersediaan memiliki ketersediaan dan toleransi kesalahan yang lebih baik, dan dapat diskalakan dibandingkan infrastruktur pusat data tunggal atau multi tradisional.

Untuk informasi selengkapnya tentang Wilayah AWS dan Availability Zone, lihat Infrastruktur AWS Global.

Selain infrastruktur AWS global, AWS End User Messaging Social menawarkan beberapa fitur untuk membantu mendukung ketahanan data dan kebutuhan pencadangan Anda.

Keamanan Infrastruktur dalam Pesan Pengguna AWS Akhir Sosial

Sebagai layanan terkelola, AWS End User Messaging Social dilindungi oleh prosedur keamanan jaringan AWS global yang dijelaskan dalam laporan resmi Amazon Web Services: Gambaran Umum Proses Keamanan.

Anda menggunakan API panggilan yang AWS dipublikasikan untuk mengakses AWS End User Messaging Social melalui jaringan. Klien harus mendukung Transport Layer Security (TLS) 1.0 atau yang lebih baru. Kami merekomendasikan TLS data yang lebih baru. Klien juga harus mendukung cipher suites dengan Perfect Forward Secrecy (PFS) seperti (Ephemeral Diffie-Hellman) atau DHE (Elliptic Curve Ephemeral Diffie-Hellman). ECDHE Sebagian besar sistem modern seperti Java 7 dan versi lebih baru mendukung mode-mode ini.

Selain itu, permintaan harus ditandatangani menggunakan access key ID dan secret access key yang terkait dengan IAM prinsipal. Atau Anda dapat menggunakan AWS Security Token Service (AWS STS) untuk menghasilkan kredensial keamanan sementara untuk menandatangani permintaan.

Pencegahan confused deputy lintas layanan

Masalah confused deputy adalah masalah keamanan saat entitas yang tidak memiliki izin untuk melakukan suatu tindakan dapat memaksa entitas yang lebih berhak untuk melakukan tindakan tersebut. Pada tahun AWS, peniruan lintas layanan dapat mengakibatkan masalah wakil yang membingungkan. Peniruan identitas lintas layanan dapat terjadi ketika satu layanan (layanan yang dipanggil) memanggil layanan lain (layanan yang dipanggil). Layanan pemanggilan dapat dimanipulasi menggunakan izinnya untuk bertindak pada sumber daya pelanggan lain dengan cara yang seharusnya tidak dilakukannya kecuali bila memiliki izin untuk mengakses. Untuk mencegah hal ini, AWS menyediakan alat yang membantu Anda melindungi data untuk semua layanan dengan pengguna utama layanan yang telah diberi akses ke sumber daya di akun Anda.

Sebaiknya gunakan kunci konteks kondisi `aws:SourceAccount`global `aws:SourceArn`dan global dalam kebijakan sumber daya untuk membatasi izin yang diberikan Social Messaging layanan lain ke sumber daya. Gunakan `aws:SourceArn` jika Anda hanya ingin satu sumber daya dikaitkan dengan akses lintas layanan. Gunakan `aws:SourceAccount` jika Anda ingin mengizinkan sumber daya apa pun di akun tersebut dikaitkan dengan penggunaan lintas layanan.

Cara paling efektif untuk melindungi dari masalah wakil yang membingungkan adalah dengan menggunakan kunci konteks kondisi `aws:SourceArn` global dengan penuh ARN sumber daya. Jika Anda tidak tahu sumber daya penuh ARN atau jika Anda menentukan beberapa sumber daya, gunakan kunci kondisi konteks `aws:SourceArn` global dengan karakter wildcard (*) untuk bagian yang tidak diketahui dari file. ARN Misalnya, `arn:aws:social-messaging:*:123456789012:*`.

Jika `aws:SourceArn` nilainya tidak berisi ID akun, seperti bucket Amazon S3ARN, Anda harus menggunakan kedua kunci konteks kondisi global untuk membatasi izin.

Nilai `aws:SourceArn` harus ResourceDescription.

Contoh berikut menunjukkan cara menggunakan kunci konteks kondisi `aws:SourceAccount` global `aws:SourceArn` dan global di Social Messaging untuk mencegah masalah wakil yang membingungkan.

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

Praktik terbaik keamanan

AWS End User Messaging Social menyediakan sejumlah fitur keamanan untuk dipertimbangkan ketika Anda mengembangkan dan menerapkan kebijakan keamanan Anda sendiri. Praktik terbaik berikut adalah pedoman umum dan tidak mewakili solusi keamanan yang lengkap. Karena praktik terbaik ini mungkin tidak sesuai atau tidak memadai untuk lingkungan Anda, perlakukan itu sebagai pertimbangan yang bermanfaat, bukan sebagai resep.

- Membuat pengguna individual untuk setiap orang yang mengelola AWS SMS sumber daya, termasuk Anda sendiri. Jangan gunakan kredensi AWS root untuk mengelola AWS SMS sumber daya.
- Beri setiap pengguna set izin minimum yang diperlukan untuk melakukan tugas-tugasnya.

- Gunakan IAM grup untuk mengelola izin secara efektif untuk beberapa pengguna.
- Siapkan IAM identitas Anda secara rutin.

Menggunakan peran yang terhubung dengan AWS layanan untuk

AWS End User Messaging Sosial menggunakan AWS Identity and Access Management (IAM) peran terkait layanan. Peran tertaut-layanan adalah tipe peran unik yang tertaut langsung ke AWS End User Messaging Social. IAM Peran tertaut layanan ditentukan sebelumnya oleh AWS End User Messaging Social dan mencakup semua izin yang diperlukan layanan untuk menghubungi AWS layanan lainnya atas nama Anda.

Peran tertaut layanan mempermudah pengaturan AWS End User Messaging Social karena Anda tidak perlu menambahkan izin yang diperlukan secara manual. AWS End User Messaging Social menentukan izin atas peran tertaut layanan, dan jika tidak ada ketentuan lain, hanya AWS End User Messaging Social yang dapat menjalankan perannya. Izin yang ditentukan mencakup kebijakan kepercayaan dan kebijakan izin, serta bahwa kebijakan izin tidak dapat dilampirkan ke entitas lain. IAM

Anda dapat menghapus peran tertaut layanan hanya setelah menghapus sumber daya terkait terlebih dahulu. Langkah ini melindungi sumber daya Sosial Pesan Pengguna AWS Akhir karena Anda tidak dapat secara tidak sengaja menghapus izin untuk mengakses sumber daya.

Untuk informasi tentang layanan lain yang mendukung peran tertaut layanan, lihat AWS Layanan yang Bekerja bersama IAM dan mencari layanan yang memiliki Ya di kolom Peran tertaut layanan. Pilih Ya bersama tautan untuk melihat dokumentasi peran tertaut layanan untuk layanan tersebut.

Izin peran yang ditautkan dengan layanan untuk AWS End User Messaging Social

AWS End User Messaging Social menggunakan peran terkait layanan bernama AWSServiceRoleForSocialMessaging— Untuk mempublikasikan metrik dan memberikan wawasan untuk pengiriman pesan sosial Anda.

Peran AWSServiceRoleForSocialMessaging terkait layanan memercayakan layanan berikut untuk menjalankan peran tersebut:

- `social-messaging.amazonaws.com`

Kebijakan izin peran yang diberi nama AWSSocialMessagingServiceRolePolicy memungkinkan AWS End User Messaging Social untuk menyelesaikan tindakan berikut pada sumber daya yang ditentukan:

- Tindakan: `"cloudwatch:PutMetricData"` pada `all AWS resources in the AWS/SocialMessaging namespace.`

Anda harus mengonfigurasikan izin untuk mengizinkan pengguna, grup, atau peran Anda untuk membuat, mengedit, atau menghapus peran terkait layanan. Untuk informasi selengkapnya, lihat Izin peran terkait layanan di Panduan Pengguna. IAM

Untuk pembaruan kebijakan, lihatAWS End User Messaging Pembaruan sosial ke kebijakan AWS terkelola.

Membuat peran terkait layanan untuk AWS End User Messaging Social

Anda dapat menggunakan IAM konsol untuk membuat peran tertaut layanan dengan kasus penggunaan AWSEndUserMessagingSocial- Metrik. Di AWS CLI atau AWS API, buat peran terkait layanan dengan nama `social-messaging.amazonaws.com` layanan. Untuk informasi selengkapnya, lihat Membuat peran terkait layanan di IAMPanduan Pengguna. Jika Anda menghapus peran tertaut layanan ini, Anda dapat mengulang proses yang sama untuk membuat peran tersebut lagi.

Mengedit peran terkait AWS layanan untuk

AWS End User Messaging tidak mengizinkan Anda untuk mengedit peran yang AWSServiceRoleForSocialMessaging ditautkan dengan layanan. Setelah Anda membuat peran terkait layanan, Anda tidak dapat mengubah nama peran karena berbagai entitas mungkin mereferensikan peran tersebut. Namun, Anda dapat menyunting penjelasan peran menggunakan IAMIAM. Untuk informasi selengkapnya, lihat Mengedit peran terkait layanan di IAMPanduan Pengguna.

Menghapus peran terkait layanan untuk AWS End User Messaging Social

Jika Anda tidak perlu lagi menggunakan fitur atau layanan yang memerlukan peran terkait layanan, kami merekomendasikan Anda menghapus peran tersebut. Dengan begitu, Anda tidak memiliki entitas yang tidak digunakan yang tidak dipantau atau dipelihara secara aktif. Tetapi, Anda harus membersihkan sumber daya peran yang terhubung dengan layanan sebelum menghapusnya secara manual.

> **Note**
>
> Jika layanan Sosial Pesan Pengguna AWS Akhir menggunakan peran tersebut ketika Anda mencoba untuk menghapus sumber daya, penghapusan mungkin gagal. Jika hal itu terjadi, tunggu beberapa menit dan coba mengoperasikannya lagi.

Untuk menghapus Sumber daya Sosial Pesan Pengguna AWS Akhir yang digunakan oleh AWSServiceRoleForSocialMessaging

1. Hubungi `list-linked-whatsapp-business-accounts` API untuk melihat sumber daya yang Anda miliki.
2. Untuk setiap akun bisnis aplikasi whats yang ditautkan, hubungi `disassociate-whatsapp-business-account` API untuk menghapus sumber daya dari SocialMessaging layanan.
3. Verifikasi tidak ada sumber daya yang dikembalikan dengan menelepon `list-linked-whatsapp-business-accounts` API lagi.

Untuk menghapus peran terkait layanan secara manual menggunakan IAM

Gunakan IAM konsol, AWS CLI, atau AWS API untuk menghapus peran AWSServiceRoleForSocialMessaging terkait layanan. Untuk informasi selengkapnya, lihat Menghapus peran terkait layanan di Panduan Pengguna. IAM

Wilayah yang Didukung untuk Peran AWS terkait layanan sosial Peran yang terhubung dengan layanan

AWS End User Messaging memberikan dukungan dengan peran terkait layanan di semua Wilayah tempat layanan tersedia. Untuk informasi selengkapnya, lihat AWS Wilayah dan titik akhir.

Kuota untuk AWS End User Messaging Sosial

AWSAkun Anda memiliki kuota default, yang sebelumnya disebut sebagai batasan, untuk masing-masing layanan. AWS Kecuali dinyatakan lain, setiap kuota bersifat khusus per Wilayah. Anda dapat meminta peningkatan untuk beberapa kuota dan kuota lainnya tidak dapat ditingkatkan.

Untuk melihat kuota untuk AWS End User Messaging Social, buka konsol Service Quotas. Di panel navigasi, pilih AWSlayanan dan pilih AWS End User Messaging Social.

Untuk meminta peningkatan kuota, lihat Meminta Peningkatan Kuota dalam Panduan Pengguna Service Quotas. Jika kuota belum tersedia dalam Service Quotas, gunakan formulir penambahan batas.

AWSAkun Anda memiliki kuota berikut yang terkait dengan AWS End User Messaging Social.

Sumber Daya	Default
WhatsApp Akun Bisnis (WABA)	25 per wilayah

AWS End User Messaging Social mengimplementasikan kuota yang membatasi jumlah permintaan yang dapat Anda buat untuk AWS End User Messaging Social API dari Anda. Akun AWS

Operasi	Laju
SendWhatsAppMessage	1.000
PostWhatsAppMessageMedia	100
GetWhatsAppMessageMedia	100
DeleteWhatsAppMessageMedia	100
DisassociateWhatsAppBusinessAccount	10
ListWhatsAppBusinessAccount	10
TagResource	10

Operasi	Laju
UntagResourceRate	10
ListTagsForResourceRate	10

Riwayat dokumen untuk Panduan Pengguna Sosial Pesan Pengguna AWS Akhir

Tabel berikut menjelaskan dokumentasi rilis AWS untuk VM.

Perubahan	Deskripsi	Tanggal
Rilis awal	Rilis awal Panduan Pengguna Sosial Pesan Pengguna AWS Akhir	10 Oktober 2019

Terjemahan disediakan oleh mesin penerjemah. Jika konten terjemahan yang diberikan bertentangan dengan versi bahasa Inggris aslinya, utamakan versi bahasa Inggris.