aws

Guia do usuário

AWS Mensagens sociais para o usuário final

AWS Mensagens sociais para o usuário final: Guia do usuário

Table of Contents

O que é o AWS End User Messaging Social? 1
Você é um usuário de redes sociais de mensagens de usuário AWS final pela primeira vez? 1
Características do sistema social de mensagens para usuários AWS finais 2
Serviços relacionados 2
Acessando AWS o sistema social de mensagens do usuário final 2
Disponibilidade regional 3
Configurando mensagens sociais para o usuário AWS final 6
Inscreva-se para um Conta da AWS 6
Criar um usuário com acesso administrativo 6
Próximas etapas 8
Conceitos básicos 9
Inscrevendo-se para WhatsApp 9
Pré-requisitos 9
Inscreva-se pelo console 11
Próximas etapas 15
WhatsApp Conta comercial (WABA) 16
Veja um WABA 17
Adicionar um WABA 17
WhatsApp tipos de conta comercial 18
Recursos adicionais 18
Números de telefone 20
Considerações sobre o número de telefone 20
Adicionar um número de telefone 21
Pré-requisitos 21
Adicionar um número de telefone a um WABA 21
Exibir o status de um número de telefone 23
Exibir a ID de um número de telefone 24
Aumente os limites de conversação por mensagens 24
Aumentar throughput de mensagens 26
Entendendo a classificação de qualidade do número de telefone 26
Exibir a classificação de qualidade de um número de telefone 27
Modelos de mensagens 28
Usando modelos de mensagem com o WhatsApp Manager 29
Próximas etapas 29

Emparelhamento do modelo 29
Receba feedback sobre o status reduzido de um modelo 30
Status do modelo e classificação de qualidade 30
Motivos pelos quais um modelo é rejeitado 32
Destinos de mensagens e eventos 34
Adicionar um destino para o evento 34
Pré-requisitos 34
Adicione uma mensagem e um destino para o evento 35
Políticas de tópicos criptografados do Amazon SNS 36
Políticas do IAM para tópicos do Amazon SNS 37
Políticas do IAM para o Amazon Connect 38
Próximas etapas 39
Formato de mensagem e evento 39
AWS Cabeçalho do evento social de mensagens para o usuário final 40
Exemplo de WhatsApp JSON para uma mensagem de texto 40
Exemplo de WhatsApp JSON para uma mensagem de mídia 42
Mensagem de status 43
Status de mensagens 43
Recursos adicionais 43
Carregando arquivos de mídia 44
Tipos de arquivo de mídia compatíveis 46
Tipos de arquivo de mídia 46
Tipos de mensagem 49
Recursos adicionais 49
Enviar mensagens 50
Enviar uma mensagem modelo 51
Enviando uma mensagem de mídia 52
Respondendo a uma mensagem recebida 55
Alterar o status de uma mensagem para lida 55
Responda com uma reação 56
Baixe um arquivo de mídia para o Amazon S3 a partir de WhatsApp 56
Exemplo de resposta a uma mensagem 57
Pré-requisitos 57
Respondendo 57
Recursos adicionais 60
Noções básicas sobre sua fatura 61

Quando a Autenticação Internacional FeeType se aplica 65
Exemplo 1: envio de uma mensagem de modelo de marketing 66
Exemplo 2: Abrindo uma conversa de serviço 66
Códigos ISO de faturamento 67
Monitorar 81
Monitoramento com CloudWatch 81
CloudTrail troncos 82
AWS Mensagens para o usuário final Eventos de dados sociais em CloudTrail 84
AWS Mensagens para o usuário final Eventos de gerenciamento social em CloudTrail 85
AWS Mensagens para usuários finais: exemplos de eventos sociais 86
Práticas recomendadas 88
Up-to-date perfil de negócios 88
Obter permissão 88
Conteúdo de mensagem proibido 89
Fazer auditoria em suas listas de clientes 91
Ajustar seu envio com base no envolvimento 91
Enviar em momentos adequados 92
Segurança 93
Proteção de dados 94
Criptografia de dados 95
Criptografia em trânsito 95
Gerenciamento de chaves 96
Privacidade do tráfego entre redes 96
Gerenciamento de identidade e acesso 97
Público 97
Autenticar com identidades 98
Gerenciar o acesso usando políticas 102
Como o AWS End User Messaging Social funciona com o IAM 104
Exemplos de políticas baseadas em identidade 111
AWS políticas gerenciadas 115
Solução de problemas 116
Validação de conformidade 118
Resiliência 119
Segurança da infraestrutura 120
Prevenção contra o ataque do “substituto confuso” em todos os serviços 120
Práticas recomendadas de segurança 122

Uso de perfis vinculados ao serviço 122
Permissões de função vinculadas ao serviço para mensagens sociais de usuário AWS final 123
Criação de uma função vinculada ao serviço para o AWS End User Messaging Social 123
Editando uma função vinculada ao serviço para AWS End User Messaging Social 124
Excluindo uma função vinculada ao serviço para AWS End User Messaging Social 124
Regiões suportadas para funções AWS vinculadas ao serviço social de mensagens de usuário final 125
AWS PrivateLink 126
Considerações 126
Como criar um endpoint de interface 126
Crie uma política de endpoint 127
Cotas 129
Histórico de documentos 130
..... cxxxi

O que é o AWS End User Messaging Social?

AWS O End User Messaging Social, também conhecido como mensagens sociais, é um serviço de mensagens que permite que os desenvolvedores se WhatsApp integrem aos seus aplicativos. Ele fornece acesso aos recursos WhatsApp de mensagens, permitindo a criação de conteúdo interativo de marca com imagens, vídeos e botões. Ao usar esse serviço, você pode adicionar a funcionalidade WhatsApp de mensagens aos seus aplicativos junto com os canais existentes, como SMS e notificações push. Isso permite que você interaja com os clientes por meio do canal de comunicação preferido deles.

Para começar, crie uma nova Conta WhatsApp Empresarial (WABA) usando o processo de integração autoguiado no console social do AWS End User Messaging ou vincule uma WABA existente ao serviço.

Tópicos

- Você é um usuário de redes sociais de mensagens de usuário AWS final pela primeira vez?
- Características do sistema social de mensagens para usuários AWS finais
- Serviços relacionados
- Acessando AWS o sistema social de mensagens do usuário final
- Disponibilidade regional

Você é um usuário de redes sociais de mensagens de usuário AWS final pela primeira vez?

Se você é um usuário iniciante do AWS End User Messaging Social, recomendamos que comece lendo as seguintes seções:

- Configurando mensagens sociais para o usuário AWS final
- Introdução ao AWS End User Messaging Social
- Práticas recomendadas para mensagens sociais para usuários AWS finais

Características do sistema social de mensagens para usuários AWS finais

AWS O End User Messaging Social fornece os seguintes recursos e capacidades:

- Crie mensagens consistentes e reutilize o conteúdo de forma mais eficaz criando e usando modelos de mensagem. Um modelo de mensagem contém conteúdo e configurações que você deseja reutilizar nas mensagens enviadas.
- Acesso a recursos avançados de mensagens para uma experiência mais envolvente. Além de texto e mídia, você pode enviar localizações e mensagens interativas.
- Receba mensagens de texto e mídia de seus clientes.
- Crie confiança com seus clientes verificando a identidade da sua empresa por meio do Meta.

Serviços relacionados

AWS oferece outros serviços de mensagens que podem ser usados juntos em um fluxo de trabalho multicanal:

- Use mensagens SMS para o usuário AWS final para enviar mensagens SMS
- Use o envio de mensagens push para o usuário AWS final para enviar notificações push
- Use o Amazon SES para enviar e-mails

Acessando AWS o sistema social de mensagens do usuário final

Você pode acessar o AWS End User Messaging Social usando o seguinte:

AWS Console social de mensagens para o usuário final

A interface da web na qual você cria e gerencia recursos.

AWS Command Line Interface

Interaja com Serviços da AWS o uso de comandos em seu shell de linha de comando. O AWS Command Line Interface é compatível com Windows, macOS e Linux. Para obter mais informações sobre o AWS CLI, consulte o Guia AWS Command Line Interface do usuário. Você pode encontrar os comandos AWS End User Messaging Social na Referência de AWS CLI Comandos.

AWS SDKs

Se você preferir criar aplicativos usando um idioma específico APIs em vez de enviar uma solicitação por HTTP ou HTTPS, use as bibliotecas, o código de amostra, os tutoriais e outros recursos fornecidos pelo. AWS Essas bibliotecas fornecem funções básicas que automatizam tarefas, como assinar criptograficamente suas solicitações, repetir solicitações e lidar com respostas de erro. Essas funções tornam mais eficiente para você começar. Para obter mais informações, consulte Ferramentas para desenvolver AWS.

Disponibilidade regional

AWS O End User Messaging Social está disponível Regiões da AWS em várias redes sociais na América do Norte, Europa, Ásia e Oceania. Em cada região, AWS mantém várias zonas de disponibilidade. Essas zonas de disponibilidade são fisicamente isoladas umas das outras, mas são unidas por conexões de rede privadas, de baixa latência, de alta taxa de transferência e altamente redundantes. Essas zonas de disponibilidade são usadas para fornecer altos níveis de disponibilidade e redundância, além de minimizar a latência.

Para saber mais sobre Regiões da AWS, consulte Especificar qual Regiões da AWS sua conta pode usar no Referência geral da Amazon Web Services. Para obter uma lista de todas as regiões em que o AWS End User Messaging Social está atualmente disponível e o endpoint de cada região, consulte Endpoints e cotas para a API Social de AWS End User Messaging Social e os endpoints de AWS serviço na ou na tabela a Referência geral da Amazon Web Servicesseguir. Para saber mais sobre quantas zonas de disponibilidade estão disponíveis em cada região, consulte Infraestrutura global da AWS.

Disponibilidade de regiões

Nome da região	Região	Endpoint	WhatsApp Versão da API
Leste dos EUA (Norte da Virgínia)	us-east-1	social-messaging.us-east-1.amazonaws.com social-messaging-fips.us-east-1.api.aws	Versão 20 e posterior

Nome da região	Região	Endpoint	WhatsApp Versão da API
		social-messaging.us-east-1.api.aws	
Leste dos EUA (Ohio)	us-east-2	social-messaging.us-east-2.amazonaws.com social-messaging-fips.us-east-2.api.aws social-messaging.us-east-2.api.aws	Versão 20 e posterior
Oeste dos EUA (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	Versão 20 e posterior
Ásia-Pacífico (Mumbai)	ap-south-1	social-messaging.ap-south-1.amazonaws.com social-messaging.ap-south-1.api.aws	Versão 20 e posterior
Ásia-Pacífico (Singapura)	ap-southeast-1	social-messaging.ap-southeast-1.amazonaws.com social-messaging.ap-southeast-1.api.aws	Versão 20 e posterior

Nome da região	Região	Endpoint	WhatsApp Versão da API
Europa (Frankfurt)	eu-central-1	social-messaging.eu-central-1.amazonaws.com social-messaging.eu-central-1.api.aws	Versão 20 e posterior
Europa (Irlanda)	eu-west-1	social-messaging.eu-west-1.amazonaws.com social-messaging.eu-west-1.api.aws	Versão 20 e posterior
Europa (Londres)	eu-west-2	social-messaging.eu-west-2.amazonaws.com social-messaging.eu-west-1.api.aws	Versão 20 e posterior

Configurando mensagens sociais para o usuário AWS final

Antes de usar o AWS End User Messaging Social pela primeira vez, você deve concluir as etapas a seguir.

Tópicos

- Inscreva-se para um Conta da AWS
- Criar um usuário com acesso administrativo
- Próximas etapas

Inscreva-se para um Conta da AWS

Se você não tiver um Conta da AWS, conclua as etapas a seguir para criar um.

Para se inscrever em um Conta da AWS

1. Abra a https://portal.aws.amazon.com/billing/inscrição.
2. Siga as instruções online.

   Parte do procedimento de inscrição envolve receber uma chamada telefônica e inserir um código de verificação no teclado do telefone.

   Quando você se inscreve em um Conta da AWS, um Usuário raiz da conta da AWSé criado. O usuário-raiz tem acesso a todos os Serviços da AWS e recursos na conta. Como prática recomendada de segurança, atribua o acesso administrativo a um usuário e use somente o usuário-raiz para executar tarefas que exigem acesso de usuário-raiz.

AWS envia um e-mail de confirmação após a conclusão do processo de inscrição. A qualquer momento, você pode visualizar a atividade atual da sua conta e gerenciar sua conta acessando https://aws.amazon.com/e escolhendo Minha conta.

Criar um usuário com acesso administrativo

Depois de se inscrever em um Conta da AWS, proteja seu Usuário raiz da conta da AWS AWS IAM Identity Center, habilite e crie um usuário administrativo para que você não use o usuário root nas tarefas diárias.

Proteja seu Usuário raiz da conta da AWS

1. Faça login AWS Management Consolecomo proprietário da conta escolhendo Usuário raiz e inserindo seu endereço de Conta da AWS e-mail. Na próxima página, insira a senha.

   Para obter ajuda ao fazer login usando o usuário-raiz, consulte Fazer login como usuário-raiz no Guia do usuário do Início de Sessão da AWS .
2. Habilite a autenticação multifator (MFA) para o usuário-raiz.

   Para obter instruções, consulte Habilitar um dispositivo de MFA virtual para seu usuário Conta da AWS raiz (console) no Guia do usuário do IAM.

Criar um usuário com acesso administrativo

1. Habilita o Centro de Identidade do IAM.

   Para obter instruções, consulte Habilitar o AWS IAM Identity Center no Guia do usuário do AWS IAM Identity Center .
2. No Centro de Identidade do IAM, conceda o acesso administrativo a um usuário.

   Para ver um tutorial sobre como usar o Diretório do Centro de Identidade do IAM como fonte de identidade, consulte Configurar o acesso do usuário com o padrão Diretório do Centro de Identidade do IAM no Guia AWS IAM Identity Center do usuário.

Iniciar sessão como o usuário com acesso administrativo

- Para fazer login com o seu usuário do Centro de Identidade do IAM, use o URL de login enviado ao seu endereço de e-mail quando o usuário do Centro de Identidade do IAM foi criado.

  Para obter ajuda para fazer login usando um usuário do IAM Identity Center, consulte Como fazer login no portal de AWS acesso no Guia Início de Sessão da AWS do usuário.

Atribuir acesso a usuários adicionais

1. No Centro de Identidade do IAM, crie um conjunto de permissões que siga as práticas recomendadas de aplicação de permissões com privilégio mínimo.

Para obter instruções, consulte Criar um conjunto de permissões no Guia do usuário do AWS IAM Identity Center .

2. Atribua usuários a um grupo e, em seguida, atribua o acesso de autenticação única ao grupo.

   Para obter instruções, consulte Adicionar grupos no Guia do usuário do AWS IAM Identity Center .

Próximas etapas

Agora que você está preparado para trabalhar com o AWS End User Messaging Social, consulte Introdução ao AWS End User Messaging Social para criar sua conta WhatsApp comercial (WABA) ou migrar sua conta WhatsApp comercial existente.

Introdução ao AWS End User Messaging Social

Esses tópicos orientam você pelas etapas para vincular ou migrar sua conta WhatsApp comercial (WABA) para o AWS End User Messaging Social.

Tópicos

- Inscrevendo-se para WhatsApp

Inscrevendo-se para WhatsApp

Uma Conta WhatsApp Comercial (WABA) permite que sua empresa use a Plataforma WhatsApp Empresarial para enviar mensagens diretamente aos seus clientes. Todos vocês WABAs fazem parte do seu portfólio de negócios da Meta. Um WABA contém ativos voltados para o cliente, como número de telefone, modelos e perfil WhatsApp comercial. Um perfil WhatsApp comercial contém as informações de contato da sua empresa que os usuários veem. Para obter mais informações sobre contas WhatsApp comerciais, consulteWhatsApp Conta comercial (WABA) nas redes sociais de mensagens do usuário AWS final.

Siga as etapas desta seção para começar a usar o AWS End User Messaging Social. Use o processo de inscrição incorporado para criar uma nova Conta WhatsApp Empresarial (WABA) ou migrar uma WABA existente para o AWS End User Messaging Social.

Pré-requisitos

Important

Trabalhando com Meta/ WhatsApp

- Seu uso da Solução WhatsApp Empresarial está sujeito aos termos e condições dos Termos de Serviço WhatsApp Empresariais, dos Termos da Solução WhatsApp Empresarial, da Política de Mensagens WhatsApp Comerciais, das Diretrizes de WhatsApp Mensagens e de todos os outros termos, políticas ou diretrizes incorporados a eles por referência (pois cada um pode ser atualizado periodicamente).
- A Meta ou WhatsApp pode, a qualquer momento, proibir seu uso da Solução WhatsApp Empresarial.
- Você deve criar uma conta WhatsApp comercial (“WABA”) com Meta e. WhatsApp

- Você deve criar uma conta de gerente de negócios com o Meta e vinculá-la ao seu WABA.
- Você deve fornecer o controle de sua WABA para nós. A seu pedido, transferiremos o controle de seu WABA de volta para você de maneira razoável e oportuna, usando os métodos que a Meta disponibiliza para nós.
- Em conexão com o uso da Solução WhatsApp Empresarial, você não enviará nenhum conteúdo, informação ou dado que esteja sujeito à regulamentação de proteçãoand/or limitations on distribution pursuant to applicable laws and/or.
- WhatsAppOs preços de uso da Solução WhatsApp Empresarial podem ser encontrados em Preços Baseados em Conversação.

- Para criar uma conta WhatsApp comercial (WABA), sua empresa precisa de uma conta comercial meta. Verifique se sua empresa já tem uma conta Meta Business. Se você não tiver uma conta Meta Business, você pode criar uma durante o processo de inscrição.
- Para usar um número de telefone que já está em uso com o aplicativo WhatsApp Messenger ou o aplicativo WhatsApp Business, você deve excluí-lo primeiro.
- Um número de telefone que pode receber um SMS ou uma senha de uso único (OTP) de voz. O número de telefone usado para se inscrever fica associado à sua WhatsApp conta e o número de telefone é usado quando você envia mensagens. O número de telefone ainda pode ser usado para SMS, MMS e mensagens de voz.
- Se você estiver importando um WABA existente, precisará do PINs para todos os números de telefone associados ao WABA importado. Para redefinir um PIN perdido ou esquecido, siga as instruções em Atualização do PIN na Referência da API Cloud da WhatsApp Business Platform.

Os seguintes pré-requisitos devem ser atendidos para usar um tópico do Amazon SNS ou uma instância do Amazon Connect como destino de mensagens e eventos.

Tópico do Amazon SNS

- Um tópico do Amazon SNS foi criado e as permissões foram adicionadas.

> **Note**
>
> Tópicos FIFO do Amazon SNS são incompatíveis.

- (Opcional) Para usar um tópico do Amazon SNS criptografado usando AWS KMS chaves, você precisa conceder permissões sociais de mensagens de usuário AWS final à política de chaves existente.

Instância do Amazon Connect

- Uma instância do Amazon Connect foi criada e as permissões foram adicionadas.

Inscreva-se pelo console

Siga estas instruções para criar uma nova WhatsApp conta, migrar sua conta existente ou adicionar um número de telefone a uma WABA existente. Como parte do processo de inscrição, você concede ao AWS End User Messaging Social acesso à sua conta WhatsApp comercial. Você também permite que AWS o End User Messaging Social cobre suas mensagens. Para obter mais informações sobre contas WhatsApp comerciais, consulteEntendendo WhatsApp os tipos de contas comerciais.

1. Abra o console social do AWS End User Messaging em https://console.aws.amazon.com/social-messaging/.
2. Escolha Contas comerciais.
3. Na página Vincular conta comercial, escolha Iniciar portal do Facebook. Uma nova janela de login do Meta aparecerá.
4. Na janela de login do Meta, insira as credenciais da sua conta do Facebook.

   Na página da conta WhatsApp comercial, escolha Adicionar número WhatsApp de telefone. Na página Adicionar número de WhatsApp telefone, escolha Iniciar portal do Facebook. Uma nova janela de login do Meta aparecerá.
5. Na janela de login do Meta, insira as credenciais da sua conta do Facebook.
6. Como parte do processo de inscrição, você concede ao AWS End User Messaging Social acesso à sua Conta WhatsApp Empresarial (WABA). Você também permite que AWS o End User Messaging Social cobre suas mensagens. Escolha Continuar.
7. Para a conta Meta Business, escolha uma conta comercial Meta existente ou Crie uma conta Meta Business.

   a. (Opcional) Se você precisar criar uma conta Meta Business, siga estas etapas:

   b. Em Nome da empresa, insira o nome da sua empresa.

c. Para o site comercial ou a página de perfil, insira o URL do site da sua empresa ou, se sua empresa não tiver um site, insira o URL da sua página de mídia social.

d. Em País, escolha o país em que sua empresa está localizada.

e. (Opcional) Escolha Adicionar endereço e insira o endereço da sua empresa.

8. Escolha Próximo.

9. Em Escolher uma conta WhatsApp comercial, escolha uma conta WhatsApp comercial existente (WABA) ou, se precisar criar uma conta, escolha Criar uma conta WhatsApp comercial.

   Em Criar ou selecionar um perfil WhatsApp comercial, escolha um perfil WhatsApp comercial existente ou Criar um novo perfil WhatsApp comercial.

10. Escolha Próximo.

11. Em Criar um perfil comercial, insira as seguintes informações:

    - Em Nome da conta WhatsApp comercial, insira um nome para sua conta. Esse campo não é voltado para o cliente.
    - Em Nome de exibição do Perfil WhatsApp Comercial, insira o nome a ser exibido para seus clientes quando eles receberem uma mensagem sua. Recomendamos que você use o nome da sua empresa como nome de exibição. O nome é revisado pela Meta e deve estar em conformidade com as regras do nome de WhatsApp exibição. Para usar um nome de marca diferente do nome da sua empresa, deve haver uma associação publicada externamente entre sua empresa e a marca. Essa associação deve ser exibida em seu site e na marca representada pelo site do nome de exibição.

      Depois de concluir o registro, o Meta realiza uma revisão do seu nome de exibição. O Meta envia um e-mail informando se o nome de exibição foi aprovado ou rejeitado. Se seu nome de exibição for rejeitado, seu limite diário de mensagens será reduzido e você poderá ser desconectado de. WhatsApp

      > **Important**
      >
      > Para alterar seu nome de exibição, você precisa criar um ticket com o suporte do Meta.

    - Em Fuso horário, escolha o fuso horário em que a empresa está localizada.
    - Em Categoria, escolha a categoria que melhor se alinha à sua empresa. Os clientes podem ver a categoria “você” como parte de suas informações de contato.

- Em Descrição da empresa, insira uma descrição da sua empresa. Os clientes podem ver a descrição da sua empresa como parte de suas informações de contato.
- Em Site, insira o site da sua empresa. Os clientes podem ver seu site como parte de suas informações de contato.
- Escolha Próximo.

12. Em Adicionar um número de telefone para WhatsApp, insira um número de telefone para se registrar. Esse número de telefone é exibido para seus clientes quando você envia uma mensagem.
13. Em Escolha como você gostaria de verificar seu número, escolha Mensagem de texto ou Chamada telefônica.

    - Quando estiver pronto para receber o código de verificação, escolha Avançar.
    - Insira o código de verificação e escolha Avançar.

14. Depois que seu número for verificado, você pode escolher Avançar para fechar a janela do Meta.
15. Para uma conta WhatsApp comercial, expanda Tags - opcional para adicionar tags à sua conta WhatsApp comercial.

    As tags são pares de chaves e valores que você pode aplicar opcionalmente aos seus AWS recursos para controlar o acesso ou o uso. Escolha Adicionar nova tag e insira um par de valores-chave para anexar.
16. Uma conta WhatsApp comercial pode ter uma mensagem e um destino de evento para registrar eventos para a conta WhatsApp comercial e todos os recursos associados à conta WhatsApp comercial. Para habilitar o registro de eventos no Amazon SNS, incluindo o registro do recebimento de uma mensagem do cliente, você deve ativar a publicação de mensagens e eventos. Para obter mais informações, consulte Destinos de mensagens e eventos no AWS End User Messaging Social.

    > **Important**
    >
    > Para poder responder às mensagens dos clientes, você deve habilitar a publicação de mensagens e eventos.

    Na seção Detalhes do destino da mensagem e do evento, ative a publicação de eventos. Para o Amazon SNS, escolha Novo tópico padrão do Amazon SNS e insira um nome em Nome

do tópico, ou escolha Tópico padrão existente do Amazon SNS e escolha um tópico na lista suspensa Tópico arn.

17. Em Números de telefone:

    Para cada número de telefone em Números de WhatsApp telefone:

    a. Para verificação do número de telefone, insira o PIN existente ou insira um novo código PIN. Para redefinir um PIN perdido ou esquecido, siga as instruções em Atualização do PIN na Referência da API Cloud da WhatsApp Business Platform.

    b. Para configuração adicional:

        i. Para Região de localização de dados - opcionalmente, escolha uma das regiões da Meta na qual armazenar seus dados em repouso. Para obter mais informações sobre as políticas de privacidade de dados da Meta, consulte Privacidade e segurança de dados e Armazenamento local da Cloud API na WhatsApp Business Platform Cloud API Reference.

        ii. As tags são pares de chaves e valores que você pode aplicar opcionalmente aos seus AWS recursos para controlar o acesso ou o uso. Escolha Adicionar nova tag e insira um par de valores-chave para anexar.

18. Uma conta WhatsApp comercial pode ter uma mensagem e um destino de evento para registrar eventos para a conta WhatsApp comercial e todos os recursos associados à conta WhatsApp comercial. Para ativar o registro de eventos, incluindo o registro do recebimento de uma mensagem do cliente, você precisa ativar a publicação de mensagens e eventos. Para obter mais informações, consulte Destinos de mensagens e eventos no AWS End User Messaging Social.

    > **Important**
    >
    > Você deve habilitar a publicação de mensagens e eventos para poder responder às mensagens dos clientes.

    Na seção Detalhes do destino da mensagem e do evento, ative a publicação de eventos.

19. Para Tipo de destino, escolha Amazon SNS ou Amazon Connect

a. Para enviar seus eventos para um destino do Amazon SNS, insira um ARN de tópico existente em ARN de tópico. Para obter exemplos de políticas do IAM, consulte Políticas do IAM para tópicos do Amazon SNS.

b. Para Amazon Connect

   i. Para Connect instance, escolha uma instância no menu suspenso.

   ii. Para ARN da função, escolha uma das seguintes opções:

      A. Escolha a função existente do IAM — Escolha uma política existente do IAM no menu suspenso Funções existentes do IAM. Para obter exemplos de políticas do IAM, consulte Políticas do IAM para o Amazon Connect.

      B. Insira o ARN da função do IAM — Insira o ARN da política do IAM em Usar o ARN da função do IAM existente. Para obter exemplos de políticas do IAM, consulte Políticas do IAM para o Amazon Connect.

20. Para concluir a configuração, escolha Adicionar número de telefone.

Próximas etapas

Depois de concluir a inscrição, você pode começar a enviar mensagens. Quando você estiver pronto para começar a enviar mensagens em grande escala, conclua a Verificação comercial. Agora que sua conta WhatsApp comercial e suas contas sociais de mensagens de usuário AWS final estão vinculadas, consulte os tópicos a seguir:

- Saiba mais sobre o destino do evento para registrar eventos e receber mensagens.
- Saiba como criar modelos de mensagens.
- Saiba como enviar uma mensagem de texto ou de mídia.
- Saiba como receber uma mensagem.
- Saiba mais sobre contas comerciais oficiais para ter uma marca de seleção verde ao lado do seu nome de exibição e aumentar a taxa de transferência de mensagens.

WhatsApp Conta comercial (WABA) nas redes sociais de mensagens do usuário AWS final

Com uma Conta WhatsApp Empresarial (WABA), você pode usar a Plataforma WhatsApp Empresarial para enviar mensagens diretamente aos seus clientes. Todos vocês WABAs fazem parte do seu portfólio de negócios Meta. Uma conta WhatsApp comercial contém ativos voltados para o cliente, como número de telefone, modelos e informações de contato comercial. Um WABA só pode existir em um Região da AWS. Para obter mais informações sobre contas WhatsApp comerciais, consulte Contas WhatsApp comerciais na referência da API WhatsApp Business Platform Cloud.

Important

Trabalhando com Meta/ WhatsApp

- Seu uso da Solução WhatsApp Empresarial está sujeito aos termos e condições dos Termos de Serviço WhatsApp Empresariais, dos Termos da Solução WhatsApp Empresarial, da Política de Mensagens WhatsApp Comerciais, das Diretrizes de WhatsApp Mensagens e de todos os outros termos, políticas ou diretrizes incorporados a eles por referência. Eles podem ser atualizados de tempos em tempos.
- A Meta ou WhatsApp pode, a qualquer momento, proibir seu uso da Solução WhatsApp Empresarial.
- Você deve criar uma conta WhatsApp comercial (WABA) com Meta e. WhatsApp
- Você deve criar uma conta de gerente de negócios com o Meta e vinculá-la ao seu WABA.
- Você deve nos conceder o controle de sua WABA. A seu pedido, transferiremos o controle de seu WABA de volta para você de maneira razoável e oportuna, usando os métodos que a Meta disponibiliza para nós.
- Em conexão com o uso da Solução WhatsApp Empresarial, você não enviará nenhum conteúdo, informação ou dado que esteja sujeito a salvaguardas ou limitações na distribuição de acordo com as leis ou regulamentos aplicáveis.
- WhatsAppOs preços de uso da Solução WhatsApp Empresarial podem ser encontrados em https://developers.facebook.com/docs/whatsapp/pricing.

Tópicos

- Exibir uma conta WhatsApp comercial (WABA) na rede social de mensagens do usuário AWS final
- Adicionar uma conta WhatsApp comercial (WABA) na rede social de mensagens do usuário AWS final
- Entendendo WhatsApp os tipos de contas comerciais

Exibir uma conta WhatsApp comercial (WABA) na rede social de mensagens do usuário AWS final

Você pode ver o WABA associado ao seu Conta da AWS.

Para ver o WABA associado à sua conta

1. Abra o console social do AWS End User Messaging em https://console.aws.amazon.com/social-messaging/.
2. Em Contas comerciais, escolha um WABA.
3. Na guia Números de telefone, veja seu número de telefone, nome de exibição, classificação de qualidade e o número de conversas iniciadas pela empresa que você deixou para o dia.

   Na guia Destinos do evento, veja o destino do seu evento. Para editar o destino do seu evento, siga as instruções emDestinos de mensagens e eventos no AWS End User Messaging Social.

   Na guia Modelos, escolha Gerenciar modelos de mensagem para editar seus WhatsApp modelos por meio do Meta. Cada WABA tem um limite de 250 modelos.

   Na guia Tags, você pode gerenciar suas tags de recursos WABA.

Adicionar uma conta WhatsApp comercial (WABA) na rede social de mensagens do usuário AWS final

Adicione um novo WABA à sua conta se você já tiver um perfil WhatsApp comercial. Como parte da criação de um novo WABA, você deve adicionar um número de telefone ao WABA.

- Para adicionar um novo WABA à sua conta, siga as etapas em: Introdução ao AWS End User Messaging Social

- Na etapa 8, escolha seu Perfil WhatsApp comercial e, em seguida, escolha Criar uma nova conta WhatsApp comercial.

Entendendo WhatsApp os tipos de contas comerciais

Sua conta WhatsApp comercial determina como você aparece para seus clientes. Quando você cria uma WhatsApp conta, sua conta será uma conta comercial. WhatsApp tem dois tipos de contas comerciais:

- Conta comercial: WhatsApp verifica a autenticidade de cada conta na Plataforma WhatsApp Empresarial. Se uma conta comercial tiver concluído o processo de verificação comercial, o nome da empresa ficará visível para todos os usuários. Esse recurso ajuda os usuários a identificar contas comerciais verificadas em WhatsApp.
- Conta comercial oficial: além dos benefícios de uma conta comercial, uma conta comercial oficial tem um selo verde no perfil e nos cabeçalhos dos tópicos do bate-papo.

  A aprovação de uma conta comercial WhatsApp oficial (OBA) exige o fornecimento de evidências de que a empresa é bem conhecida e reconhecida pelos consumidores, como artigos, postagens em blogs ou avaliações independentes. A aprovação de WhatsApp um OBA não é garantida, mesmo que a empresa forneça a documentação necessária. O processo de aprovação está sujeito à análise e aprovação por WhatsApp. WhatsApp não divulga publicamente os critérios específicos que eles usam para avaliar e aprovar solicitações de contas comerciais oficiais. As empresas que buscam WhatsApp um OBA devem demonstrar sua reputação e reconhecimento, mas a aprovação final fica a critério da. WhatsApp

Quando você cria uma WhatsApp conta, sua conta será uma conta comercial. Você pode fornecer informações aos seus clientes sobre sua empresa, como site, endereço e horário. Para empresas que não concluíram a Verificação WhatsApp Comercial, o nome de exibição é mostrado em texto pequeno ao lado do número de telefone na visualização de contatos, não na lista de bate-papo ou no bate-papo individual. Depois que a verificação do Meta Business for concluída, o nome de exibição do WhatsApp remetente será mostrado na lista de bate-papo e nos tópicos de bate-papo individuais.

Recursos adicionais

- Para obter mais informações sobre a conta comercial e a conta comercial oficial, consulte Contas comerciais na referência da API de nuvem da WhatsApp Business Platform.

- Para obter mais informações sobre o processo de verificação comercial, consulte Verificação comercial na referência da API WhatsApp Business Platform Cloud.

Números de telefone no AWS End User Messaging Social

Todas as contas WhatsApp comerciais contêm um ou mais números de telefone usados para verificar sua identidade WhatsApp e são usados como parte de sua identidade de envio. Você pode ter vários números de telefone associados a uma conta WhatsApp comercial (WABA) e usar cada número de telefone para uma marca diferente.

Tópicos

- Considerações sobre o número de telefone para uso com uma WhatsApp conta comercial
- Adicionar um número de telefone a uma conta WhatsApp comercial (WABA)
- Exibir o status de um número de telefone
- Exibir o ID de um número de telefone no AWS End User Messaging Social
- Aumente os limites de conversação de mensagens em WhatsApp
- Aumente a taxa de transferência de mensagens em WhatsApp
- Compreendendo a classificação de qualidade do número de telefone em WhatsApp

Considerações sobre o número de telefone para uso com uma WhatsApp conta comercial

Ao vincular um número de telefone à sua conta WhatsApp comercial (WABA), considere o seguinte:

- Os números de telefone só podem ser vinculados a um WABA por vez.
- O número de telefone ainda pode ser usado para SMS, MMS e chamadas de voz.
- Cada número de telefone tem uma classificação de qualidade da Meta.

Você pode obter um número de telefone compatível com SMS por meio do AWS End User Messaging SMS fazendo o seguinte:

1. Verifique se o país ou a região do número de telefone suporta SMS bidirecional.
2. Solicite o número de telefone. Dependendo do país ou da região, talvez seja necessário registrar o número de telefone.
3. Ative mensagens SMS bidirecionais para o número de telefone. Quando a configuração estiver concluída, suas mensagens SMS recebidas serão enviadas para o destino do evento.

Adicionar um número de telefone a uma conta WhatsApp comercial (WABA)

Você pode adicionar números de telefone a uma conta WhatsApp comercial existente (WABA) ou criar uma nova WABA para o número de telefone.

Pré-requisitos

Antes de começar, os seguintes pré-requisitos devem ser atendidos:

- O número de telefone deve ser capaz de receber um SMS ou uma senha de uso único (OTP) de voz. Esse é o número de telefone que é adicionado ao seu WABA.
- O número de telefone não deve estar associado a nenhum outro WABA.

Os seguintes pré-requisitos devem ser atendidos para usar um tópico do Amazon SNS ou uma instância do Amazon Connect como destino de mensagem e evento.

Tópico do Amazon SNS

- Um tópico do Amazon SNS foi criado e as permissões foram adicionadas.

> **Note**
>
> Tópicos FIFO do Amazon SNS são incompatíveis.

- (Opcional) Para usar um tópico do Amazon SNS criptografado usando AWS KMS chaves, você precisa conceder permissões sociais de mensagens de usuário AWS final à política de chaves existente.

Instância do Amazon Connect

- Uma instância do Amazon Connect foi criada e as permissões foram adicionadas.

Adicionar um número de telefone a um WABA

Para adicionar um novo número de telefone ao seu WABA existente

1. Abra o console social do AWS End User Messaging em https://console.aws.amazon.com/social-messaging/.
2. Escolha Contas comerciais e, em seguida, Adicionar número de WhatsApp telefone.
3. Na página Adicionar número de WhatsApp telefone, escolha Iniciar portal do Facebook. Uma nova janela de login do Meta aparecerá.
4. Na janela de login do Meta, insira as credenciais da sua conta de desenvolvedor do Meta e escolha seu portfólio de negócios.
5. Escolha o WABA e o Perfil WhatsApp Comercial aos quais você deseja adicionar o número de telefone.
6. Escolha Próximo.
7. Em Adicionar um número de telefone para WhatsApp, insira um número de telefone para se registrar. Esse número de telefone é exibido para seus clientes quando você envia uma mensagem.
8. Em Escolha como você gostaria de verificar seu número, escolha Mensagem de texto ou Chamada telefônica.
9. Quando estiver pronto para receber o código de verificação, escolha Avançar
10. Insira o código de verificação e escolha Avançar. Depois que seu número for verificado, você pode escolher Avançar para fechar a janela do Meta.
11. Em Números de WhatsApp telefone:

    a. Para verificação do número de telefone, insira o PIN existente ou insira um novo código PIN. Para redefinir um PIN perdido ou esquecido, siga as instruções em Atualização do PIN na Referência da API Cloud da WhatsApp Business Platform.

    b. Para configuração adicional:

        i. Para Região de localização de dados - opcional, escolha uma das regiões da Meta na qual armazenar seus dados em repouso. Para obter mais informações sobre as políticas de privacidade de dados da Meta, consulte Privacidade e segurança de dados e Armazenamento local da Cloud API na WhatsAppBusiness Platform Cloud API Reference.

        ii. As tags são pares de chaves e valores que você pode aplicar opcionalmente aos seus AWS recursos para controlar o acesso ou o uso. Escolha Adicionar nova tag e insira um par de valores-chave para anexar.
12. Uma conta WhatsApp comercial pode ter uma mensagem e um destino de evento para registrar eventos para a conta WhatsApp comercial e todos os recursos associados à conta

WhatsApp comercial. Para ativar o registro de eventos, incluindo o registro do recebimento de uma mensagem do cliente, ative a publicação de mensagens e eventos. Para obter mais informações, consulte Destinos de mensagens e eventos no AWS End User Messaging Social.

> **Important**
>
> Você deve habilitar a publicação de mensagens e eventos para poder responder às mensagens dos clientes.

Na seção Detalhes do destino da mensagem e do evento, ative a publicação de eventos.

13. Para Tipo de destino, escolha Amazon SNS ou Amazon Connect

    a. Para enviar seus eventos para um destino do Amazon SNS, insira um ARN de tópico existente em ARN de tópico. Para obter exemplos de políticas do IAM, consulte Políticas do IAM para tópicos do Amazon SNS.

    b. Para Amazon Connect

        i. Para Connect instance, escolha uma instância no menu suspenso.

        ii. Para a função de canal bidirecional, escolha uma das seguintes opções:

            A. Escolha a função existente do IAM — Escolha uma política existente do IAM no menu suspenso Funções existentes do IAM. Para obter exemplos de políticas do IAM, consulte Políticas do IAM para o Amazon Connect.

            B. Insira o ARN da função do IAM — Insira o ARN da política do IAM em Usar o ARN da função do IAM existente. Para obter exemplos de políticas do IAM, consulte Políticas do IAM para o Amazon Connect.

14. Para concluir a configuração, escolha Adicionar número de telefone.

Exibir o status de um número de telefone

Para poder enviar mensagens no AWS End User Messaging Social, o status do número de telefone deve ser Ativo.

1. Abra o console social do AWS End User Messaging em https://console.aws.amazon.com/social-messaging/.
2. Selecione Phone numbers (Números de telefone).

3. Na seção Números de telefone, a coluna Status tem o status de cada número de telefone.

> **Note**
>
> Se o status de um número de telefone for Configuração incompleta, você poderá escolher o número de telefone e, em seguida, escolher Configuração completa para concluir a configuração do número de telefone.

Exibir o ID de um número de telefone no AWS End User Messaging Social

Para poder enviar mensagens com o AWS CLI, você precisa do ID do número de telefone para identificar o número de telefone a ser usado ao enviar.

1. Abra o console social do AWS End User Messaging em https://console.aws.amazon.com/social-messaging/.
2. Selecione Phone numbers (Números de telefone).
3. Na seção Números de telefone, selecione um número.
4. A seção Detalhes do número de telefone contém o ID do número de telefone.

Aumente os limites de conversação de mensagens em WhatsApp

Os limites de conversação se referem ao número máximo de conversação iniciada pela empresa que um número de telefone comercial pode abrir em um período de 24 horas. Inicialmente, os números de telefone comerciais são limitados a 250 conversas iniciadas pela empresa em um período de mudança de 24 horas. Esse limite pode ser aumentado pelo Meta com base na classificação de qualidade de suas mensagens e na quantidade de mensagens que você envia. As conversas iniciadas pela empresa só podem usar mensagens modelo.

Quando um cliente envia uma mensagem para você, isso abre uma janela de atendimento de 24 horas. Durante esse período, você pode enviar todos os tipos de mensagens.

Você pode aumentar seu limite de mensagens para 1.000 mensagens sozinho seguindo estas diretrizes:

- Seu número de telefone comercial deve ter um status Ativo.

- Se o número de telefone da sua empresa tiver uma classificação de qualidade baixa, ele poderá continuar limitado a 250 conversas iniciadas pela empresa por dia até que o índice de qualidade melhore.
- Inscreva-se para a verificação comercial. Se sua empresa for aprovada, a qualidade das mensagens será analisada para determinar se sua atividade de mensagens justifica um aumento no limite de mensagens. Com base na análise, sua solicitação de aumento do limite de mensagens será aprovada ou negada pela Meta.
- Inscreva-se para verificação de identidade. Se você concluir a verificação de identidade e sua identidade for confirmada, a Meta aprovará um aumento no limite de mensagens.
- Abra 1.000 ou mais conversas iniciadas por empresas em um período de mudança de 30 dias usando um modelo com uma classificação de alta qualidade. Depois de atingir o limite de 1.000 conversas, a qualidade das mensagens será analisada para determinar se sua atividade de mensagens justifica um aumento no limite de mensagens. O objetivo é enviar mensagens de alta qualidade de forma consistente para potencialmente aumentar seu limite de mensagens.

Se você concluiu a Verificação Comercial ou a Verificação de Identidade, ou abriu 1.000 ou mais conversas comerciais, e ainda está limitado a 250 conversas iniciadas pela empresa, envie uma solicitação à Meta para uma atualização do nível de mensagens.

Se sua verificação comercial ou de identidade for rejeitada, você poderá aumentar suas chances de ser aprovado enviando mensagens de alta qualidade. Ao enviar mensagens de alta qualidade, compatíveis e opcionais, sua atividade e qualidade de mensagens podem ser reavaliadas, potencialmente levando a um aumento em seus recursos de mensagens aprovados.

Seu índice de qualidade de mensagens WhatsApp é calculado com base nos comentários e interações recentes dos usuários, com mais peso atribuído aos dados mais recentes. Isso ajuda a avaliar a qualidade geral e a confiabilidade de suas mensagens na plataforma.

Aumento do nível de limites de mensagens

- 1.000 conversas iniciadas por empresas
- 10 mil conversas iniciadas por empresas
- 100 mil conversas iniciadas por empresas
- Um número ilimitado de conversas iniciadas por empresas

Aumente a taxa de transferência de mensagens em WhatsApp

A taxa de transferência de mensagens é o número de mensagens recebidas e enviadas por segundo (MPS) para um número de telefone. Por padrão, cada número MPS de telefone tem 80. O Meta pode aumentar seu MPS para 1.000 se você atender às seguintes condições:

- O número de telefone deve ser capaz de enviar um número ilimitado de conversas iniciadas pela empresa
- O número de telefone deve ter uma classificação de qualidade média ou superior.

Compreendendo a classificação de qualidade do número de telefone em WhatsApp

A qualidade do seu número de telefone e mensagens é determinada pelo Meta. Seu índice de qualidade de mensagens é baseado em como suas mensagens foram recebidas pelos clientes nos últimos sete dias, com as mensagens mais recentes tendo um peso maior. O índice de qualidade das mensagens é calculado com base em uma combinação de sinais de qualidade das conversas entre você e seus WhatsApp usuários. Esses sinais incluem feedback do usuário, como bloqueios, relatórios e os motivos que os usuários fornecem quando bloqueiam uma empresa. O Meta avalia a qualidade de suas mensagens com base em quão bem elas são recebidas por seus clientes WhatsApp, com foco nos comentários e interações recentes.

WhatsApp classificações de qualidade do número de telefone

- Verde: Alta qualidade
- Amarelo: qualidade média
- Vermelho: Baixa qualidade

WhatsApp status do número de telefone

- Conectado: você pode enviar mensagens dentro da sua cota de mensagens.
- Sinalizado: a qualidade do seu número de telefone está baixa e precisa ser melhorada. Se sua qualidade não melhorar em sete dias, o status do seu número de telefone será alterado para Conectado, mas o limite de conversas iniciadas pela empresa será reduzido em um nível.

- Restrito: você atingiu o limite de conversas iniciadas pela empresa no período atual de 24 horas. Você ainda pode responder às mensagens recebidas. Quando o período de 24 horas terminar, você poderá enviar mensagens novamente.

Exibir a classificação de qualidade de um número de telefone

Siga estas instruções para ver a qualidade dos números de telefone.

1. Abra o console social do AWS End User Messaging em https://console.aws.amazon.com/social-messaging/.
2. Em Contas comerciais, escolha uma Conta WhatsApp comercial (WABA).
3. Na guia Números de telefone, veja seu número de telefone, nome de exibição, classificação de qualidade e o número de conversas iniciadas pela empresa que você deixou para o dia.

Usando modelos de mensagem no AWS End User Messaging Social

> **Important**
>
> A partir de 01/04/2025, o Meta bloqueará os modelos de mensagens de marketing enviados para o código de país dos EUA de. +1 Para obter mais informações, consulte Limites de mensagens do modelo de marketing por usuário na WhatsAppBusiness Platform Cloud API Reference.

Você pode usar modelos de mensagem para tipos de mensagem que você usa com frequência, como boletins semanais ou lembretes de compromissos. As mensagens modelo são o único tipo de mensagem que pode ser enviada aos clientes que ainda não enviaram mensagens para você ou que não enviaram uma mensagem nas últimas 24 horas.

O Meta atribui a cada modelo uma classificação de qualidade e um status. A classificação de qualidade afeta o status de um modelo e diminui o ritmo ou a taxa de envio de um modelo.

Os modelos são associados à sua conta WhatsApp comercial (WABA), gerenciados pelo WhatsApp gerente e revisados por WhatsApp.

Você pode enviar os seguintes tipos de modelo:

- Baseado em texto
- Baseado em mídia
- Mensagem interativa
- Baseado na localização
- Modelos de autenticação com botões de senha de uso único
- Modelos de mensagens para vários produtos

O Meta fornece modelos de amostra pré-aprovados. Para saber mais, consulte Exemplos de modelos de mensagem.

Para obter mais informações sobre os tipos de modelos de mensagem, consulte Modelo de mensagem na WhatsApp Business Platform Cloud API Reference.

Usando modelos de mensagem com o WhatsApp Manager

Use o WhatsAppGerenciador para criar, modificar ou verificar o status de um modelo.

1. Abra o console social de mensagens para usuários AWS finais em https://console.aws.amazon.com/social-messaging/.
2. Escolha Conta comercial e, em seguida, escolha uma WABA.
3. Na guia Modelos de mensagem, escolha Gerenciar modelos de mensagem. O WhatsAppgerenciador é aberto em uma nova janela na qual você pode gerenciar seus modelos escolhendo Modelos de mensagem.

Próximas etapas

Depois de criar ou editar um modelo, você deve enviá-lo para análise com WhatsApp. A revisão do Meta pode levar até 24 horas. O Meta envia um e-mail para o administrador do seu Business Manager e atualiza o status do modelo no WhatsApp gerenciador. Use o WhatsAppgerenciador para verificar o status do seu modelo.

Entendendo o ritmo dos modelos em WhatsApp

O ritmo de modelos é um método usado pela Meta que permite o feedback antecipado do cliente sobre modelos novos ou modificados. Ele identifica e pausa modelos que recebem pouco engajamento ou feedback, dando a você tempo para ajustar o conteúdo do modelo antes de enviá-lo para muitos clientes. Isso reduz o risco de o feedback negativo do cliente afetar os negócios. Por exemplo, se muitos clientes “bloquearem” sua mensagem ou se seu modelo tiver baixas taxas de leitura, a classificação de qualidade do modelo poderá ser reduzida.

O ritmo dos modelos afeta modelos recém-criados, modelos que não foram pausados e modelos sem uma classificação de alta qualidade. O ritmo dos modelos geralmente é iniciado por um histórico anterior de modelos pausados ou de baixa qualidade. Quando um modelo é embalado, as mensagens que usam esse modelo são enviadas normalmente até um determinado limite determinado pelo Meta. Depois disso, as mensagens subsequentes são retidas para dar tempo ao feedback do cliente. Se o feedback for positivo, o ritmo do modelo será então ampliado. Se o feedback for negativo, o ritmo do modelo será reduzido, permitindo que você ajuste o conteúdo do modelo. Para obter mais informações, consulte Ritmo de modelos na Referência da API Cloud da WhatsApp Business Platform.

Obtenha feedback sobre o status reduzido de um modelo com o Manager WhatsApp

O Meta fornece informações sobre o motivo pelo qual o status de um modelo foi reduzido. Use o feedback do Meta para editar o modelo e enviá-lo para reaprovação, usar um modelo diferente ou alterar o comportamento do seu aplicativo. Se você editar o modelo de mensagem e ele for reaprovado, sua classificação de qualidade melhorará gradualmente, desde que não receba feedback negativo frequente ou baixas taxas de leitura.

1. Abra o console social de mensagens para usuários AWS finais em https://console.aws.amazon.com/social-messaging/.
2. Escolha Conta comercial e, em seguida, escolha uma WABA.
3. Na guia Modelos de mensagem, escolha Gerenciar modelos de mensagem. O WhatsAppgerente abre em uma nova janela.
4. Escolha Modelos de mensagem e passe o mouse sobre o modelo. Uma dica de ferramenta deve aparecer com feedback sobre por que a classificação foi reduzida.

Entendendo o status e a classificação de qualidade de um modelo no WhatsApp

Cada modelo de mensagem recebe uma classificação de qualidade com base no uso, no feedback do cliente e no engajamento do cliente. Um modelo só pode ser usado se o status for Ativo, mas a qualidade determina o ritmo do modelo. Se um modelo de mensagem receber feedback negativo de forma consistente ou apresentar baixo engajamento, isso causará uma alteração no status do modelo.

O Meta altera automaticamente o status ou a classificação de qualidade de um modelo com base no feedback negativo ou positivo e no engajamento. Se o status do seu modelo mudar, você receberá uma notificação WhatsApp do gerente, um e-mail e uma notificação de evento. Use o WhatsAppgerenciador para verificar o status do seu modelo.

Se seu modelo for rejeitado por WhatsApp, você poderá editá-lo e reenviá-lo para aprovação ou registrar uma apelação com WhatsApp. Para saber mais, consulte Apelações na Referência da API Cloud da WhatsApp Business Platform.

Status do modelo	Classificação de qualidade	Significado
Em análise		O modelo da mensagem está sendo revisado. Isso pode levar até 24 horas para ser concluído.
Rejeitado		O modelo de mensagem foi rejeitado e você pode entrar com uma apelação.
Ativo	Pendente	O modelo de mensagem não recebeu feedback de qualidade nem informações de taxa de leitura dos clientes, mas o modelo ainda pode ser usado para enviar mensagens .
Ativo	Alto	O modelo de mensagem recebeu pouco ou nenhum feedback negativo do cliente e pode ser usado para enviar mensagens.
Ativo	Médio	O modelo de mensagem recebeu feedback negativo dos clientes ou baixas taxas de leitura e pode estar pausado ou desativado.
Ativo	Baixo	O modelo de mensagem recebeu feedback negativo dos clientes ou baixas taxas de leitura. Modelos de mensagem com esse status podem ser usados,

Status do modelo	Classificação de qualidade	Significado
		mas correm o risco de serem pausados ou desativados. Quando um modelo passa para o status Ativo-Baixo, seu envio é pausado. A primeira pausa é de três horas, a segunda pausa é de seis horas e a próxima pausa desativa o modelo.
Paused		O modelo de mensagem foi pausado devido ao feedback negativo recorrente dos clientes ou às baixas taxas de leitura.
Desabilitado		O modelo de mensagem foi desativado devido ao feedback negativo recorrente dos clientes.
Recurso solicitado		Uma apelação foi solicitada.

Razões pelas quais um modelo é rejeitado no WhatsApp

Se seu modelo de mensagem for revisado e rejeitado pelo Meta, você receberá um e-mail explicando por que o modelo foi rejeitado. Você pode contestar a rejeição ou modificar seu modelo de mensagem. Esses são alguns dos motivos comuns pelos quais o Meta pode rejeitar um modelo de mensagem:

- Os parâmetros variáveis contêm caracteres especiais, como #, $ ou%.
- Os parâmetros variáveis estão ausentes, têm colchetes incompatíveis ou não são sequenciais.
- O modelo de mensagem contém conteúdo que viola a Política WhatsApp Comercial ou a Política WhatsApps Comercial.

Para obter mais informações, consulte Motivos comuns de rejeição na referência da WhatsApp Business Platform Cloud API.

Destinos de mensagens e eventos no AWS End User Messaging Social

O destino de um evento é um tópico do Amazon SNS ou uma instância do Amazon Connect para a qual os WhatsApp eventos são enviados. Quando você ativa a publicação de eventos, todos os seus eventos de envio e recebimento são enviados para o destino da mensagem e do evento. Use eventos para monitorar, rastrear e analisar o status das mensagens enviadas e das comunicações recebidas com os clientes.

Cada conta WhatsApp comercial (WABA) pode ter um destino de evento. Todos os eventos de todos os recursos associados à Conta WhatsApp Comercial são registrados no destino do evento. Por exemplo, você pode ter uma conta WhatsApp comercial com três números de telefone associados a ela e todos os eventos desses números de telefone são registrados no destino de um evento.

Tópicos

- Adicionar um destino de mensagem e evento ao AWS End User Messaging Social
- Formato de mensagem e evento no AWS End User Messaging Social
- WhatsApp status

Adicionar um destino de mensagem e evento ao AWS End User Messaging Social

Quando você ativa a publicação de mensagens e eventos, todos os eventos gerados pela sua conta WhatsApp comercial (WABA) são enviados para o tópico do Amazon SNS. Isso inclui eventos para cada número de telefone associado a uma conta WhatsApp comercial. Seu WABA pode ter um tópico do Amazon SNS associado a ele.

Pré-requisitos

Antes de começar, os seguintes pré-requisitos devem ser atendidos para usar um tópico do Amazon SNS ou uma instância do Amazon Connect como destino de mensagens e eventos.

Tópico do Amazon SNS

- Um tópico do Amazon SNS foi criado e as permissões foram adicionadas.

> **Note**
>
> Tópicos FIFO do Amazon SNS são incompatíveis.

- (Opcional) Para usar um tópico do Amazon SNS criptografado usando AWS KMS chaves, você precisa conceder permissões sociais de mensagens de usuário AWS final à política de chaves existente.

Instância do Amazon Connect

- Uma instância do Amazon Connect foi criada e as permissões foram adicionadas.

Adicione uma mensagem e um destino para o evento

1. Abra o console social do AWS End User Messaging em https://console.aws.amazon.com/social-messaging/.
2. Escolha Conta comercial e, em seguida, escolha uma WABA.
3. Na guia Destino do evento, escolha Editar destino.
4. Para ativar o destino de um evento, escolha Habilitar.
5. Para Tipo de destino, escolha Amazon SNS ou Amazon Connect

    a. Para enviar seus eventos para um destino do Amazon SNS, insira um ARN de tópico existente em ARN de tópico. Para obter exemplos de políticas do IAM, consulte Políticas do IAM para tópicos do Amazon SNS.

    b. Para Amazon Connect

        i. Para Connect instance, escolha uma instância no menu suspenso.

        ii. Para a função de canal bidirecional, escolha uma das seguintes opções:

            A. Escolha a função existente do IAM — Escolha uma política existente do IAM no menu suspenso Funções existentes do IAM. Para obter exemplos de políticas do IAM, consulte Políticas do IAM para o Amazon Connect.

            B. Insira o ARN da função do IAM — Insira o ARN da política do IAM em Usar o ARN da função do IAM existente. Para obter exemplos de políticas do IAM, consulte Políticas do IAM para o Amazon Connect.

6. Escolha Salvar alterações.

Políticas de tópicos criptografados do Amazon SNS

Você pode usar tópicos do Amazon SNS que são criptografados usando AWS KMS chaves para obter um nível adicional de segurança. Essa segurança adicional pode ser útil se seu aplicativo manipula dados privados ou confidenciais. Para obter mais informações sobre a criptografia de tópicos do Amazon SNS AWS KMS usando chaves, consulte Habilitar a compatibilidade entre fontes de eventos AWS de serviços e tópicos criptografados no Guia do desenvolvedor do Amazon Simple Notification Service.

> **Note**
>
> Tópicos FIFO do Amazon SNS são incompatíveis.

A declaração de exemplo usa as `SourceArn` condições opcionais, mas recomendadas, `SourceAccount` para evitar o confuso problema adjunto, e somente a conta do proprietário do AWS End User Messaging Social tem acesso. Para obter mais informações sobre o problema do deputado confuso, consulte O problema do deputado confuso no guia do usuário do IAM.

A chave que você usa deve ser simétrica. Tópicos criptografados do Amazon SNS não oferecem suporte a chaves AWS KMS assimétricas.

A política de chaves deve ser modificada para permitir que o AWS End User Messaging Social use a chave. Siga as instruções em Alteração de uma política de chaves, no Guia do AWS Key Management Service desenvolvedor, para adicionar as seguintes permissões à política de chaves existente:

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

Políticas do IAM para tópicos do Amazon SNS

Para usar uma função do IAM existente ou criar uma nova função, anexe a política a seguir a essa função para que o AWS End User Messaging Social possa assumi-la. Para obter informações sobre como modificar a relação de confiança de uma função, consulte Modificar uma função no guia do usuário do IAM.

Veja a seguir a política de permissão para a função do IAM. A política de permissão permite a publicação em tópicos do Amazon SNS.

Na política de permissão do IAM a seguir, faça as seguintes alterações:

- *{PARTITION}*Substitua pela AWS partição na qual você usa o AWS End User Messaging Social.
- *{REGION}*Substitua por Região da AWS aquela em que você usa o AWS End User Messaging Social.
- *{ACCOUNT}*Substitua pelo ID exclusivo do seu Conta da AWS.
- *{TOPIC_NAME}*Substitua pelos tópicos do Amazon SNS que receberão mensagens.

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

Políticas do IAM para o Amazon Connect

Se você quiser que o AWS End User Messaging Social use uma função existente do IAM ou se você criar uma nova função, anexe as seguintes políticas a essa função para que o AWS End User Messaging Social possa assumi-la. Para obter informações sobre como modificar uma relação de confiança existente de uma função, consulte Modificar uma função no guia do usuário do IAM. Essa função é usada tanto para enviar eventos quanto para importar números de telefone do AWS End User Messaging Social para o Amazon Connect.

Para criar novas políticas do IAM, faça o seguinte:

1. Crie uma nova política de permissão seguindo as instruções em Como criar políticas usando o editor JSON no Guia do usuário do IAM.

    - Na etapa 5, use a política de permissão para a função do IAM para permitir a publicação no Amazon Connect.

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

2. Crie uma nova política de confiança seguindo as instruções em Como criar uma função usando políticas de confiança personalizadas no Guia do usuário do IAM.

   a. Na etapa 4, use a política de confiança para a função do IAM.

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

   b. Na etapa 10, adicione a política de permissão que você criou na etapa anterior.

Próximas etapas

Depois de configurar seu tópico do Amazon SNS, você deve inscrever um endpoint para o tópico. O endpoint começará a receber mensagens publicadas no tópico associado. Para obter mais informações sobre a assinatura de um tópico, consulte Assinatura de um tópico do Amazon SNS no Guia do desenvolvedor do Amazon SNS.

Formato de mensagem e evento no AWS End User Messaging Social

O objeto JSON de um evento contém o cabeçalho do AWS evento e a carga WhatsApp JSON. Para ver uma lista da carga e dos valores da WhatsApp notificação JSON, consulte Referência da carga útil de notificação de Webhooks e Status da mensagem na Referência da API Cloud da WhatsApp Business Platform.

AWS Cabeçalho do evento social de mensagens para o usuário final

O objeto JSON de um evento contém o cabeçalho do AWS evento e o WhatsApp JSON. O cabeçalho contém os AWS identificadores ARNs de sua conta WhatsApp comercial (WABA) e número de telefone.

```
{
  "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
}
```

No evento de exemplo anterior:

- *1234567890abcde*é o ID WABA da Meta.
- *abcde1234567890*é o ID do número de telefone da Meta.
- *fb2594b8a7974770b128a409e2example*é o ID da conta WhatsApp comercial (WABA).
- *976c72a700aac43eaf573ae050example*é o ID do número de telefone.

Exemplo de WhatsApp JSON para receber uma mensagem de texto

O seguinte mostra o registro do evento de uma mensagem de texto recebida de WhatsApp. O JSON é gerado por WhatsApp. Para ver uma lista dos campos e seus significados, consulte Referência de carga útil de notificação de webhooks na Referência da API de nuvem da WhatsApp Business Platform.

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

Exemplo de WhatsApp JSON para receber uma mensagem de mídia

O seguinte mostra o registro do evento para uma mensagem de mídia recebida. Para recuperar o arquivo de mídia, use o comando da GetWhatsAppMessageMedia API. Para obter uma lista de campos e seus significados, consulte Referência de carga útil de notificação de webhooks


```
{
//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

Ao enviar uma mensagem, você recebe atualizações de status sobre a mensagem. Você precisa ativar o registro de eventos para receber essas notificações, consulteDestinos de mensagens e eventos no AWS End User Messaging Social.

Status de mensagens

A tabela a seguir contém os possíveis status de mensagens.

Nome do status	Descrição
deleted	O cliente excluiu a mensagem e você também deve excluir a mensagem se ela tiver sido baixada para o seu servidor.
entregue	A mensagem foi entregue com êxito ao cliente.
com falha	A mensagem falhou ao ser enviada.
leitura	O cliente leu a mensagem. Esse status só é enviado se o cliente tiver os recibos de leitura ativados.
enviado	A mensagem foi enviada, mas ainda está em trânsito.
aviso	A mensagem contém um item que não está disponível ou não existe.

Recursos adicionais

Para obter mais informações, consulte Status da mensagem na WhatsApp Business Platform Cloud API Reference.

Carregando arquivos de mídia para enviar WhatsApp

Quando você envia ou recebe um arquivo de mídia, ele precisa ser armazenado em um bucket do Amazon S3 e carregado ou recuperado. WhatsApp O bucket do Amazon S3 deve estar no mesmo Conta da AWS e Região da AWS na sua conta WhatsApp comercial (WABA). Essas instruções mostram como criar um bucket do Amazon S3, fazer upload de um arquivo e criar a URL para o arquivo. Para obter mais informações sobre os comandos do Amazon S3, consulte Usar comandos de alto nível (s3) com a AWS CLI. Para obter mais informações sobre como configurar o AWS CLI, consulte Configurar a AWS CLI no Guia AWS Command Line Interface do usuário e Criar um bucket e fazer upload de objetos no Guia do usuário do Amazon S3.

> **Note**
>
> WhatsApp armazena arquivos de mídia por 30 dias antes de excluí-los, consulte Carregar mídia na Referência da API Cloud da WhatsApp Business Platform.

Você também pode criar uma URL pré-assinada para o arquivo de mídia. Com um URL pré-assinado, você pode conceder acesso por tempo limitado aos objetos e carregá-los sem exigir que outra pessoa tenha credenciais ou permissões AWS de segurança.

1. Para criar um bucket do Amazon S3, use o comando AWS CLI create-bucket. Na linha de comando, insira o seguinte comando:

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

   No comando anterior:

   - *us-east-1*Substitua pelo em Região da AWS que seu WABA está.
   - *BucketName*Substitua pelo nome do novo bucket.

2. Para copiar um arquivo para o bucket do Amazon S3, use o comando cp AWS CLI . Na linha de comando, insira o seguinte comando:

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

   No comando anterior:

- *SourceFilePathAndName*Substitua pelo caminho do arquivo e pelo nome do arquivo a ser copiado.
- Substitua *BucketName* pelo nome do bucket.
- *FileName*Substitua pelo nome a ser usado no arquivo.

O URL a ser usado ao enviar é:

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

Para criar um URL pré-assinado, substitua-o por suas próprias informações. *user input placeholders*

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

O URL retornado será: `https://amzn-s3-demo-bucket1.s3.af-south-1.amazonaws.com/mydoc.txt?{Headers}`

3. Faça upload do arquivo de mídia WhatsApp usando o post-whatsapp-message-mediacomando. Após a conclusão bem-sucedida, o comando retornará o*{MEDIA_ID}*, que é necessário para enviar a mensagem de mídia.

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

No comando anterior, faça o seguinte:

- *{ORIGINATION_PHONE_NUMBER_ID}*Substitua pelo ID do seu número de telefone.
- *{BUCKET}*Substitua pelo nome do bucket do Amazon S3.
- *{MEDIA_FILE}*Substitua pelo nome do arquivo de mídia.

Você também pode fazer o upload usando um URL predefinido usando `--source-s3-presigned-url` em vez de`--source-s3-file`. Você deve adicionar `Content-Type` no `headers` campo. Se você usar os dois, um `InvalidParameterException` será retornado.

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

4. Após a conclusão bem-sucedida, o *MEDIA_ID* é retornado. O *MEDIA_ID* é usado para referenciar o arquivo de mídia ao enviar uma mensagem de mídia.

Tipos e tamanhos de arquivos de mídia suportados em WhatsApp

Ao enviar ou receber uma mensagem de mídia, o tipo de arquivo deve ser compatível e estar abaixo do tamanho máximo do arquivo. Para obter mais informações, consulte Tipos de mídia compatíveis na WhatsApp Business Platform Cloud API Reference.

Tipos de arquivo de mídia

Formatos de áudio

Tipo de áudio	Extensão	Tipo MIME	Tamanho máximo
AAC	.aac	áudio/aac	16 MB
AMR	.amr	áudio/amr	16 MB
MP3	.mp3	audio/mpeg	16 MB
MP4 Áudio	.m4a	áudio/mp4	16 MB
Áudio OGG	.ogg	audio/ogg	16 MB

Formatos de documentos

Tipo de documento	Extensão	Tipo MIME	Tamanho máximo
Texto	.texto	text/plain	100 MB
Microsoft Excel	.xls, .xlsx	application/vnd.ms-excel, application/vnd.openxmlform	100 MB

Tipo de documento	Extensão	Tipo MIME	Tamanho máximo
		ats-officedocument .spreadsheetml.sheet	
Microsoft Word	.doc, .docx	application/msword , application/vnd.op enxmlformats-offic edocument.wordproc essingml.document	100 MB
Microsoft PowerPoint	.ppt, .pptx	application/vnd.ms- powerpoint, applicati on/vnd.openxmlform ats-officedocument .presentationml.pr esentation	100 MB
PDF	.pdf	application/pdf	100 MB

Formatos de imagem

Tipo de imagem	Extensão	Tipo MIME	Tamanho máximo
JPEG	.jpeg	image/jpeg	5 MB
PNG	.png	image/png	5 MB

Formatos de adesivos

Tipo de adesivo	Extensão	Tipo MIME	Tamanho máximo
Adesivo animado	.webp	imagem/webp	500 KB
Adesivo estático	.webp	imagem/webp	100 KB

Formatos de vídeo

Tipo de vídeo	Extensão	Tipo MIME	Tamanho máximo
3GPP	.3gp	vídeo/3gp	16 MB
MP4 Vídeo	.mp4	vídeo/mp4	16 MB

WhatsApp tipos de mensagem

Este tópico lista os tipos de mensagens compatíveis e uma descrição de seu uso. Para ver uma lista dos tipos de mensagens, consulte Mensagens na Referência da API Cloud da WhatsApp Business Platform.

Tipo de mensagem	Descrição
Texto	Envie uma mensagem de texto ou URL para seu cliente.
Mídia	Envie um arquivo de áudio, documento, imagem, adesivo ou vídeo. Você também pode enviar links do arquivo de mídia.
Reaction	Envie um emoji como reação a uma mensagem, como um polegar para cima.
Modelo	Envie uma mensagem modelo.
Local	Envie uma localização.
Contatos	Envie um cartão de contato.
Interativo	Envie uma mensagem interativa.

Recursos adicionais

Para ver uma lista de objetos de WhatsApp mensagem, consulte Mensagens na Referência da API Cloud da WhatsApp Business Platform.

Envio de mensagens por meio WhatsApp do AWS End User Messaging Social

Antes de enviar uma mensagem, você deve configurar sua Conta WhatsApp Comercial (WABA) e seu usuário deve optar por receber mensagens suas. Para obter mais informações, consulte Obter permissão.

Quando um usuário envia uma mensagem para você, um cronômetro de 24 horas chamado janela de atendimento ao cliente é iniciado ou atualizado. Todos os tipos de mensagem, exceto as mensagens modelo, só podem ser enviados quando uma janela de atendimento ao cliente está aberta entre você e o usuário. As mensagens modelo podem ser enviadas a qualquer momento, desde que o usuário tenha optado por receber mensagens suas.

Para cada mensagem que você envia ou recebe, um status de mensagem é gerado e enviado para o destino do evento. Se seu cliente não se inscreveu WhatsApp, um evento é gerado com o status da mensagem `defail`. Você deve ativar um destino de mensagem e evento para receber o status da mensagem.

Para ver uma lista dos tipos de mensagens, consulte Mensagens na Referência da API Cloud da WhatsApp Business Platform.

> **Important**
>
> Trabalhando com Meta/ WhatsApp
>
> - Seu uso da Solução WhatsApp Empresarial está sujeito aos termos e condições dos Termos de Serviço WhatsApp Empresariais, dos Termos da Solução WhatsApp Empresarial, da Política de Mensagens WhatsApp Comerciais, das Diretrizes de WhatsApp Mensagens e de todos os outros termos, políticas ou diretrizes incorporados a eles por referência. Eles podem ser atualizados de tempos em tempos.
> - A Meta ou WhatsApp pode, a qualquer momento, proibir seu uso da Solução WhatsApp Empresarial.
> - Em conexão com o uso da Solução WhatsApp Empresarial, você não enviará nenhum conteúdo, informação ou dado que esteja sujeito a salvaguardas ou limitações na distribuição de acordo com as leis ou regulamentos aplicáveis.

Tópicos

- Exemplo de envio de uma mensagem modelo no AWS End User Messaging Social
- Exemplo de envio de uma mensagem de mídia no AWS End User Messaging Social

Exemplo de envio de uma mensagem modelo no AWS End User Messaging Social

Para obter mais informações sobre os tipos de modelos de mensagem que podem ser enviados, consulte Modelo de mensagem na WhatsApp Business Platform Cloud API Reference. Para ver uma lista dos tipos de mensagens que podem ser enviadas, consulte Mensagens na Referência da API Cloud da WhatsApp Business Platform.

O exemplo a seguir mostra como usar um modelo para enviar uma mensagem ao seu cliente usando AWS CLI o. Para obter mais informações sobre como configurar o AWS CLI, consulte Configurar o AWS CLI no Guia do AWS Command Line Interface Usuário.

> **Note**
>
> Você deve especificar a codificação base64 ao usar a AWS CLI versão 2. Isso pode ser feito adicionando o AWS CLI parâmetro `--cli-binary-format raw-in-base64-out` ou alterando o arquivo de configuração AWS CLI global. Para obter mais informações, consulte `cli_binary_format`o Guia do usuário da interface de linha de AWS comando para a versão 2.

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

No comando anterior, faça o seguinte:

- *{PHONE_NUMBER}*Substitua pelo número de telefone do seu cliente.
- *{ORIGINATION_PHONE_NUMBER_ID}*Substitua pelo ID do seu número de telefone.

O exemplo a seguir mostra como enviar uma mensagem modelo que não contém nenhum componente.

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

- *{PHONE_NUMBER}*Substitua pelo número de telefone do seu cliente.
- *{ORIGINATION_PHONE_NUMBER_ID}*Substitua pelo ID do seu número de telefone.

Exemplo de envio de uma mensagem de mídia no AWS End User Messaging Social

O exemplo a seguir mostra como enviar uma mensagem de mídia para seu cliente usando AWS CLI o. Para obter mais informações sobre como configurar o AWS CLI, consulte Configurar o AWS CLI no Guia do AWS Command Line Interface Usuário. Para obter uma lista dos tipos de arquivos de mídia compatíveis, consulteTipos e tamanhos de arquivos de mídia suportados em WhatsApp.

> **Note**
>
> WhatsApp armazena arquivos de mídia por 30 dias antes de excluí-los, consulte Carregar mídia na Referência da API Cloud da WhatsApp Business Platform.

1. Faça o upload do arquivo de mídia em um bucket do Amazon S3. Para obter mais informações, consulte Carregando arquivos de mídia para enviar WhatsApp.
2. Faça upload do arquivo de mídia WhatsApp usando o post-whatsapp-message-mediacomando. Após a conclusão bem-sucedida, o comando retornará o*{MEDIA_ID}*, que é necessário para enviar a mensagem de mídia.

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

   No comando anterior, faça o seguinte:

- *{ORIGINATION_PHONE_NUMBER_ID}*Substitua pelo ID do seu número de telefone.
- *{BUCKET}*Substitua pelo nome do bucket do Amazon S3.
- *{MEDIA_FILE}*Substitua pelo nome do arquivo de mídia.

Você também pode fazer o upload usando um URL predefinido usando `--source-s3-presigned-url` em vez de`--source-s3-file`. Você deve adicionar `Content-Type` no `headers` campo. Se você usar os dois, um `InvalidParameterException` será retornado.

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

3. Use o send-whatsapp-messagecomando para enviar a mensagem de mídia.

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

> **Note**
>
> Você deve especificar a codificação base64 ao usar a AWS CLI versão 2. Isso pode ser feito adicionando o AWS CLI parâmetro `--cli-binary-format raw-in-base64-out` ou alterando o arquivo de configuração AWS CLI global. Para obter mais informações, consulte `cli_binary_format`o Guia do usuário da interface de linha de AWS comando para a versão 2.
>
> ```
> aws socialmessaging send-whatsapp-message --message
>  '{"messaging_product":"whatsapp","to":"'{PHONE_NUMBER}'","type":"image","image":
> {"id":"'{MEDIA_ID}'"}}' --origination-phone-number-
> id {ORIGINATION_PHONE_NUMBER_ID} --meta-api-version v20.0 --cli-binary-
> format raw-in-base64-out
> ```

No comando anterior, faça o seguinte:

- *{PHONE_NUMBER}*Substitua pelo número de telefone do seu cliente.
- *{ORIGINATION_PHONE_NUMBER_ID}*Substitua pelo ID do seu número de telefone.

- *{MEDIA_ID}*Substitua pela ID da mídia retornada da etapa anterior.

4. Quando você não precisar mais do arquivo de mídia, poderá excluí-lo WhatsApp usando o delete-whatsapp-message-mediacomando. Isso remove apenas o arquivo de mídia do bucket do Amazon S3, WhatsApp e não do seu bucket.

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

No comando anterior, faça o seguinte:

- *{ORIGINATION_PHONE_NUMBER_ID}*Substitua pelo ID do seu número de telefone.
- *{MEDIA_ID}*Substitua pela ID da mídia.

Respondendo a uma mensagem no AWS End User Messaging Social

Antes de receber uma mensagem de texto ou de mídia, você deve ter configurado sua Conta WhatsApp Empresarial (WABA) e um destino para o evento. Quando você recebe uma mensagem, um evento é salvo no tópico Amazon SNS de destino do evento. Para receber uma notificação, você deve se inscrever no endpoint de tópicos do Amazon SNS.

Para obter um exemplo de evento de uma mensagem de mídia recebida, consulteExemplo de WhatsApp JSON para receber uma mensagem de mídia. Para obter mais informações sobre como configurar o AWS CLI, consulte Configurar o AWS CLI no Guia do AWS Command Line Interface Usuário. Para obter uma lista dos tipos de arquivos de mídia compatíveis, consulteTipos e tamanhos de arquivos de mídia suportados em WhatsApp.

> **Important**
>
> Para receber mensagens recebidas, você deve ter os destinos de eventos habilitados para o WABA. Para obter mais informações, consulte Adicionar um destino de mensagem e evento ao AWS End User Messaging Social.

Exemplo de alteração do status de uma mensagem para lida no AWS End User Messaging Social

Você pode definir o status da mensagem para mostrar `read` ao usuário final duas marcas de seleção azuis na tela.

```
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
```

No comando anterior, faça o seguinte:

- *{ORIGINATION_PHONE_NUMBER_ID}*Substitua pelo ID do seu número de telefone.
- *{MESSAGE_ID}*Substitua pelo identificador exclusivo da mensagem. Use o valor do `id` campo no objeto de mensagem do tópico do Amazon SNS.

Exemplo de resposta a uma mensagem com uma reação no AWS End User Messaging Social

Você pode adicionar uma reação à mensagem, como um polegar para cima.

```
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
```

No comando anterior, faça o seguinte:

- *{PHONE_NUMBER}*Substitua pelo número de telefone do seu cliente.
- *{MESSAGE_ID}*Substitua pelo identificador exclusivo da mensagem. Use o valor do `id` campo no objeto de mensagem do tópico do Amazon SNS.
- *{ORIGINATION_PHONE_NUMBER_ID}*Substitua pelo ID do seu número de telefone.

Baixe um arquivo de mídia WhatsApp para o Amazon S3

Para recuperar um arquivo de mídia e salvá-lo em um bucket do Amazon S3, use get-whatsapp-message-mediao comando.

```
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
}
```

No comando anterior, faça o seguinte:

- *{BUCKET}*Substitua pelo nome do bucket do Amazon S3.
- *{MEDIA_ID}*Substitua pelo valor do `id` campo do evento recebido. Para ver um exemplo de evento de mídia recebido, consulteExemplo de WhatsApp JSON para receber uma mensagem de mídia.
- *{ORIGINATION_PHONE_NUMBER_ID}*Substitua pelo ID do seu número de telefone.

Para recuperar a mídia do bucket do Amazon S3, use o seguinte comando:

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

No comando anterior, faça o seguinte:

- *{BUCKET}*Substitua pelo nome do bucket do Amazon S3.
- *{MEDIA_ID}*Substitua pelo MEDIA_ID retornado da etapa anterior.

Exemplo de resposta a uma mensagem com confirmação de leitura e reação

Neste exemplo, seu cliente, Diego, enviou uma mensagem dizendo “Oi” e você responde com um recibo de leitura e um emoji de aceno manual.

Pré-requisitos

Para receber uma notificação de que Diego enviou uma mensagem, você deve ter configurado um SNS tópico da Amazon de destino para o evento e se inscrito em um endpoint de tópico.

Respondendo

1. Quando a mensagem de Diego é recebida, um evento é publicado nos pontos finais do tópico. A seguir está um trecho do que o tópico publica.

   > **Note**
   >
   > Como Diego iniciou a conversa, ela não conta na cota das conversas iniciadas pela sua empresa.

   ```
   {
     "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. Para mostrar a Diego que você recebeu a mensagem, defina o status como`read`. Diego verá duas marcas de verificação azuis ao lado da mensagem em seu dispositivo.

> **Note**
>
> Você deve especificar a codificação base64 ao usar a AWS CLI versão 2. Isso pode ser feito adicionando o AWS CLI parâmetro `--cli-binary-format raw-in-base64-out` ou alterando o arquivo de configuração AWS CLI global. Para obter mais informações, consulte `cli_binary_format`o Guia do usuário da interface de linha de AWS comando para a versão 2.

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

No comando anterior, faça o seguinte:

- Substituir *{ORIGINATION_PHONE_NUMBER_ID}* com o número de telefone para o qual Diego enviou sua mensagem`phone-number-id-976c72a700aac43eaf573ae050example`.
- Substituir *{MESSAGE_ID}* com o identificador exclusivo da mensagem. Esse é o mesmo valor do `id` campo na mensagem recebida`wamid.HBgLMTQyNTY5ODgzMDIVAgASGCBDNzBDRjM5MDU2ODEwMDkwREY4ODBDRDE0RjV`

3. Você pode enviar a Diego uma reação de aceno manual.

```
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
```

No comando anterior, faça o seguinte:

- Substituir *{PHONE_NUMBER}* com o número de telefone de Diego,`14255550150`.

- Substituir *{MESSAGE_ID}* com o identificador exclusivo da mensagem. Esse é o mesmo valor do `id` campo na mensagem recebidawamid.HBgLMTQyNTY5ODgzMDIVAgASGCBDNzBDRjM5MDU2ODEwMDkwREY4ODBDRDE0RjV
- Substituir *{ORIGINATION_PHONE_NUMBER_ID}* com o número de telefone para o qual Diego enviou sua mensagem:`phone-number-id-976c72a700aac43eaf573ae050example`.

Recursos adicionais

- Permita que os destinos dos eventos registrem eventos e recebam mensagens.
- Para obter uma lista de objetos de WhatsApp mensagem, consulte Mensagens na WhatsApp Business Platform Cloud API Reference.

Entendendo os relatórios WhatsApp de faturamento e uso do AWS End User Messaging Social

O canal social AWS End User Messaging gera um tipo de uso que contém cinco campos no seguinte formato:*Region code*-*MessagingType*-*ISO*-*FeeDescription*-*FeeType*. Há dois itens de cobrança possíveis para cada WhatsApp conversa: a WhatsApp`ConversationFee`, e a AWS por`MessageFee`.

Quando você inicia uma conversa enviando uma mensagem modelo, você é cobrado por uma WhatsApp `ConversationFee` e uma AWS por. `MessageFee` Isso abre uma janela de 24 horas em que cada mensagem que você envia ou recebe do mesmo cliente é cobrada como uma AWS por cada`MessageFee`.

O tipo de WhatsApp conversa e os detalhes de preços podem ser encontrados em Preços baseados em conversas no Guia do desenvolvedor da plataforma WhatsApp de negócios.

A tabela a seguir exibe os valores e descrições possíveis para os campos no tipo de uso. Para obter mais informações sobre preços sociais de mensagens para usuários AWS finais, consulte WhatsAppPreços de mensagens para usuários AWS finais.

Campo	Opções	Descrição
Region code	• USE1— Região Leste dos EUA (Norte da Virgínia) • USE2— Região Leste dos EUA (Ohio) • USW1— Região Oeste dos EUA (Oregon) • APS1— Região Ásia-Pacífico (Mumbai) • APSE1— Região Ásia-Pacífico (Singapura) • EUW1— Região Europa (Irlanda)	O Região da AWS prefixo que indica de onde a WhatsApp mensagem foi enviada ou recebida.

Campo	Opções	Descrição
	• EUW2— Região Europa (Londres)	
MessagingType	`WhatsApp`	Esse campo identifica o tipo de mensagem que está sendo enviada.
ISO	Veja os países com suporte	O código ISO de dois dígitos do país para o qual a mensagem foi enviada.
FeeDescription	`ConversationFee` , `MessageFee`	Esse campo especifica o WhatsApp `ConversationFee` ou o AWS por. `MessageFee`

Campo	Opções	Descrição
FeeType	`Authentication` , `Authentication-International` , `Marketing` , `Service`, `Utility`, `Standard`	Esse campo exibe o tipo de conversa que foi usado ou especifica o padrão para a taxa por mensagem **`ConversationFee`** Categorias iniciadas por negócios • `Marketing` — Usado para atingir uma ampla gama de metas, desde gerar conscientização até impulsionar vendas e retargeting de clientes. Os exemplos incluem anúncios de novos produtos, serviços ou recursos, promoções /ofertas direcionadas e lembretes de abandono do carrinho. • `Utility`— Usado para acompanhar as ações ou solicitações do usuário. Os exemplos incluem confirmação opcional, gerenciamento de pedidos/entregas (por exemplo, uma atualização de entrega); atualizações ou alertas da conta (por exemplo, um lembrete de pagamento); ou pesquisas de feedback. • `Authentication` — Usado para autentica

Campo	Opções	Descrição
		r usuários com senhas de uso único, potencialmente em várias etapas do processo de login (por exemplo, verificação de conta, recuperação de conta e desafios de integridade). • `Authentication-International` — Usado da mesma forma que `Authentication`, mas sua empresa está qualificada para tarifas de autenticação internacional, com base em outro país, e a conversa foi aberta no horário de início ou após o horário de início do país. • `Service` — Usado para resolver dúvidas de clientes. **`ConversationFee`** Categorias iniciadas pelo usuário • `Service` — Usado para resolver dúvidas de clientes. Categorias de **`MessageFee`** • `Standard` — Taxa por mensagem enviada ou recebida.

Quando você inicia uma conversa enviando uma mensagem modelo, você é cobrado por um `ConversationFee` e um. `MessageFee` Isso abre uma janela de 24 horas em que cada modelo de mensagem que você envia para o mesmo cliente é cobrado individualmente`MessageFee`. Durante a janela de 24 horas, as mensagens modelo devem ser do mesmo tipo ou uma nova conversa será iniciada.

Por exemplo, se você enviar uma mensagem de modelo de marketing para um cliente, você será cobrado pelo `ConversationFee` e. `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
```

Se o cliente enviar uma mensagem e você responder, você será cobrado pela abertura de uma nova `Service` conversa e mensagem.

```
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
```

Quando a Autenticação Internacional FeeType se aplica

Para obter uma lista de países com um `Authentication-International` FeeType, consulte Preços WhatsAppde mensagens para usuários AWS finais.

Se você abrir uma `Authentication` conversa com um WhatsApp usuário cujo código de chamada do país tenha um `Authentication-International` FeeType, a `Authentication-International` tarifa desse país será cobrada se:

1. Sua empresa abre mais de 750 mil conversas em um período móvel de 30 dias em todas as suas contas WhatsApp comerciais com WhatsApp usuários cujos códigos de chamada de país são de um país que tem uma tarifa. `Authentication-International` Para obter mais informações, consulte Elegibilidade no Guia do desenvolvedor da plataforma de WhatsApp negócios.

> **Important**
>
> Se a Meta determinar que sua empresa está qualificada`Authentication-International`, ela tentará enviar uma notificação por e-mail com os países aplicáveis e os horários de início do período de 30 dias.

2. Sua empresa está sediada em outro país. Para obter mais informações sobre como gerenciar a localização da sua empresa, consulte Local principal da empresa no Guia do desenvolvedor da plataforma de WhatsApp negócios.
3. A conversa foi aberta em ou após seu horário de início naquele país

Exemplo 1: envio de uma mensagem de modelo de marketing

Por exemplo, se você enviar uma mensagem de modelo de marketing para um cliente, você será cobrado por uma WhatsApp `ConversationFee` e uma AWS por`MessageFee`.

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

Exemplo 2: Abrindo uma conversa de serviço

Uma taxa de conversação de serviço se aplica quando uma empresa responde à mensagem de entrada de um usuário que está fora de qualquer janela de conversação ativa de 24 horas iniciada pela empresa. Nesse cenário, você é cobrado um WhatsApp `ConversationFee` e um AWS `MessageFee` por cada mensagem de entrada e saída.

```
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 Mensagens para o usuário final, faturamento social, códigos ISO e mapeamento da taxa de WhatsApp conversação

Países com suporte

Código de país ISO de dois dígitos	Nome do país	WhatsApp região de cobrança da conversa
AF	Afghanistan	Rest of Asia Pacific
AX	Aland Islands	Other
AL	Albania	Rest of Central & Eastern Europe
DZ	Algeria	Rest of Africa
AS	American Samoa	Other
AD	Andorra	Other
AO	Angola	Rest of Africa
AI	Anguilla	Other
AQ	Antarctica	Other
AG	Antigua and Barbuda	Other
AR	Argentina	Argentina
AM	Armenia	Rest of Central & Eastern Europe
AW	Aruba	Other
AC	Ascension Island	Other
AU	Australia	Rest of Asia Pacific
AT	Austria	Rest of Western Europe

Código de país ISO de dois dígitos	Nome do país	WhatsApp região de cobrança da conversa
AZ	Azerbaijan	Rest of Central & Eastern Europe
BS	Bahamas	Other
BH	Bahrain	Rest of Middle East
BD	Bangladesh	Rest of Asia Pacific
BB	Barbados	Other
BY	Belarus	Rest of Central & Eastern Europe
BE	Belgium	Rest of Western Europe
BZ	Belize	Other
BJ	Benin	Rest of Africa
BM	Bermuda	Other
BT	Bhutan	Other
BO	Bolivia	Rest of Latin America
BQ	Bonaire	Other
BA	Bosnia and Herzegovina	Other
BW	Botswana	Rest of Africa
BV	Bouvet Island	Other
BR	Brazil	Brazil
IO	British Indian Ocean Territory	Other
VG	British Virgin Islands	Other

Código de país ISO de dois dígitos	Nome do país	WhatsApp região de cobrança da conversa
BN	Brunei Darussalam	Other
BG	Bulgaria	Rest of Central & Eastern Europe
BF	BurkinaFaso	Rest of Africa
BI	Burundi	Rest of Africa
KH	Cambodia	Rest of Asia Pacific
CM	Cameroon	Rest of Africa
CA	Canada	North America
CV	Cape Verde	Other
KY	Cayman Islands	Other
CF	Central African Republic	Other
TD	Chad	Rest of Africa
CL	Chile	Chile
CN	China	Rest of Asia Pacific
CX	Christmas Island	Other
CC	Cocos(Keeling) Islands	Other
CO	Colombia	Colombia
KM	Comoros	Other
CK	Cook Islands	Other
CR	Costa Rica	Rest of Latin America

Código de país ISO de dois dígitos	Nome do país	WhatsApp região de cobrança da conversa
CI	Cote d'Ivoire	Rest of Africa
HR	Croatia	Rest of Central & Eastern Europe
CW	Curacao	Other
CY	Cyprus	Other
CZ	Czech Republic	Rest of Central & Eastern Europe
CD	Democratic Republic of the Congo	Rest of Africa
DK	Denmark	Rest of Western Europe
DJ	Djibouti	Other
DM	Dominica	Other
DO	Dominican Republic	Rest of Latin America
EC	Ecuador	Rest of Latin America
EG	Egypt	Egypt
SV	El Salvador	Rest of Latin America
GQ	Equatorial Guinea	Other
ER	Eritrea	Rest of Africa
EE	Estonia	Other
ET	Ethiopia	Rest of Africa
SZ	Eswatini	Rest of Africa

Código de país ISO de dois dígitos	Nome do país	WhatsApp região de cobrança da conversa
FK	Falkland Islands	Other
FO	Faroe Islands	Other
FJ	Fiji	Other
FI	Finland	Rest of Western Europe
FR	France	France
GF	French Guiana	Other
PF	French Polynesia	Other
TF	French Southern Territories	Other
GA	Gabon	Rest of Africa
GM	Gambia	Rest of Africa
GE	Georgia	Rest of Central & Eastern Europe
DE	Germany	Germany
GH	Ghana	Rest of Africa
GI	Gibraltar	Other
GR	Greece	Rest of Central & Eastern Europe
GL	Greenland	Other
GD	Grenada	Other
GP	Guadeloupe	Other
GU	Guam	Other

Código de país ISO de dois dígitos	Nome do país	WhatsApp região de cobrança da conversa
GT	Guatemala	Rest of Latin America
GG	Guernsey	Other
GN	Guinea	Other
GW	Guinea-Bissau	Rest of Africa
GY	Guyana	Other
HT	Haiti	Rest of Latin America
HM	Heard and McDonald Islands	Other
HN	Honduras	Rest of Latin America
HK	Hong Kong	Rest of Asia Pacific
HU	Hungary	Rest of Central & Eastern Europe
IS	Iceland	Other
IN	India	India
ID	Indonesia	Indonesia
IQ	Iraq	Rest of Middle East
IE	Ireland	Rest of Western Europe
IM	Isle of Man	Other
IL	Israel	Israel
IT	Italy	Italy
JM	Jamaica	Rest of Latin America

Código de país ISO de dois dígitos	Nome do país	WhatsApp região de cobrança da conversa
JP	Japan	Rest of Asia Pacific
JE	Jersey	Other
JO	Jordan	Rest of Middle East
KZ	Kazakhstan	Other
KE	Kenya	Rest of Africa
KI	Kiribati	Other
XK	Kosovo	Other
KW	Kuwait	Rest of Middle East
KG	Kyrgyzstan	Other
LA	Lao PDR	Rest of Asia Pacific
LV	Latvia	Rest of Central & Eastern Europe
LB	Lebanon	Rest of Middle East
LS	Lesotho	Rest of Africa
LR	Liberia	Rest of Africa
LY	Libya	Rest of Africa
LI	Liechtenstein	Other
LT	Lithuania	Rest of Central & Eastern Europe
LU	Luxembourg	Other
MO	Macao	Other

Código de país ISO de dois dígitos	Nome do país	WhatsApp região de cobrança da conversa
MK	Macedonia	Rest of Central & Eastern Europe
MG	Madagascar	Rest of Africa
MW	Malawi	Rest of Africa
MY	Malaysia	Malaysia
MV	Maldives	Other
ML	Mali	Rest of Africa
MT	Malta	Other
MH	Marshall Islands	Other
MQ	Martinique	Other
MR	Mauritania	Rest of Africa
MU	Mauritius	Other
YT	Mayotte	Other
MX	Mexico	Mexico
FM	Micronesia	Other
MD	Moldova	Rest of Central & Eastern Europe
MC	Monaco	Other
MN	Mongolia	Rest of Asia Pacific
ME	Montenegro	Other
MS	Montserrat	Other

Código de país ISO de dois dígitos	Nome do país	WhatsApp região de cobrança da conversa
MA	Morocco	Rest of Africa
MZ	Mozambique	Rest of Africa
MM	Myanmar	Other
NA	Namibia	Rest of Africa
NR	Nauru	Other
NP	Nepal	Rest of Asia Pacific
NL	Netherlands	Netherlands
NC	New Caledonia	Other
NZ	New Zealand	Rest of Asia Pacific
NI	Nicaragua	Rest of Latin America
NE	Niger	Rest of Africa
NG	Nigeria	Nigeria
NU	Niue	Other
NF	Norfolk Island	Other
MP	Northern Mariana Islands	Other
NO	Norway	Rest of Western Europe
OM	Oman	Rest of Middle East
PK	Pakistan	Pakistan
PW	Palau	Other
PS	Palestinian Territory	Other

Código de país ISO de dois dígitos	Nome do país	WhatsApp região de cobrança da conversa
PA	Panama	Rest of Latin America
PG	Papua New Guinea	Rest of Asia Pacific
PY	Paraguay	Rest of Latin America
PE	Peru	Peru
PH	Philippines	Rest of Asia Pacific
PN	Pitcairn	Other
PL	Poland	Rest of Central & Eastern Europe
PT	Portugal	Rest of Western Europe
PR	Puerto Rico	Rest of Latin America
QA	Qatar	Rest of Middle East
CG	Republic of Congo	Other
RE	Reunion	Other
RO	Romania	Rest of Central & Eastern Europe
RU	Russian Federation	Russia
RW	Rwanda	Rest of Africa
SH	Saint Helena	Other
KN	Saint Kitts and Nevis	Other
LC	Saint Lucia	Other
PM	Saint Pierre and Miquelon	Other

Código de país ISO de dois dígitos	Nome do país	WhatsApp região de cobrança da conversa
VC	Saint Vincent and Grenadines	Other
BL	Saint-Barthelemy	Other
MF	Saint-Martin	Other
WS	Samoa	Other
SM	San Marino	Other
ST	Sao Tome and Principe	Other
SA	Saudi Arabia	Saudi Arabia
SN	Senegal	Rest of Africa
RS	Serbia	Rest of Central & Eastern Europe
SC	Seychelles	Other
SL	Sierra Leone	Rest of Africa
SG	Singapore	Rest of Asia Pacific
SX	Sint Maarten	Other
SK	Slovakia	Rest of Central & Eastern Europe
SI	Slovenia	Rest of Central & Eastern Europe
SB	Solomon Islands	Other
SO	Somalia	Rest of Africa
ZA	South Africa	South Africa

Código de país ISO de dois dígitos	Nome do país	WhatsApp região de cobrança da conversa
GS	South Georgia and the South Sandwich Islands	Other
KR	South Korea	Other
SS	South Sudan	Rest of Africa
ES	Spain	Spain
LK	Sri Lanka	Rest of Asia Pacific
SR	Suriname	Other
SJ	Svalbard and Jan Mayen Islands	Other
SE	Sweden	Rest of Western Europe
CH	Switzerland	Rest of Western Europe
TW	Taiwan	Rest of Asia Pacific
TJ	Tajikistan	Rest of Asia Pacific
TZ	Tanzania	Rest of Africa
TH	Thailand	Rest of Asia Pacific
TL	Timor-Leste	Other
TG	Togo	Rest of Africa
TK	Tokelau	Other
TO	Tonga	Other
TT	Trinidad and Tobago	Other
TA	Tristan da Cunha	Other

Código de país ISO de dois dígitos	Nome do país	WhatsApp região de cobrança da conversa
TN	Tunisia	Rest of Africa
TR	Turkey	Turkey
TM	Turkmenistan	Rest of Asia Pacific
TC	Turks and Caicos Islands	Other
TV	Tuvalu	Other
UG	Uganda	Rest of Africa
UA	Ukraine	Rest of Central & Eastern Europe
AE	United Arab Emirates	United Arab Emirates
GB	United Kingdom	United Kingdom
US	United States	North America
UY	Uruguay	Rest of Latin America
UM	US Minor Outlying Islands	Other
UZ	Uzbekistan	Rest of Asia Pacific
VU	Vanuatu	Other
VA	Vatican City State	Other
VE	Venezuela	Rest of Latin America
VN	Vietnam	Rest of Asia Pacific
VI	Virgin Islands	Other
WF	Wallis and Futuna Islands	Other

Código de país ISO de dois dígitos	Nome do país	WhatsApp região de cobrança da conversa
EH	Western Sahara	Other
YE	Yemen	Rest of Middle East
ZM	Zambia	Rest of Africa
ZW	Zimbabwe	Other

Monitorando as mensagens sociais do usuário AWS final

O monitoramento é uma parte importante da manutenção da confiabilidade, disponibilidade e desempenho do AWS End User Messaging Social e de suas outras AWS soluções. AWSfornece as seguintes ferramentas de monitoramento para monitorar o AWS End User Messaging Social, relatar quando algo está errado e realizar ações automáticas quando apropriado:

- A Amazon CloudWatch monitora seus AWS recursos e os aplicativos em que você executa AWS em tempo real. É possível coletar e rastrear métricas, criar painéis personalizados e definir alarmes que o notificam ou que realizam ações quando uma métrica especificada atinge um limite definido. Por exemplo, você pode CloudWatch rastrear o CPU uso ou outras métricas de suas EC2 instâncias da Amazon e iniciar automaticamente novas instâncias quando necessário. Para obter mais informações, consulte o Guia CloudWatch do usuário da Amazon.
- O Amazon CloudWatch Logs permite que você monitore, armazene e acesse seus arquivos de log de EC2 instâncias da Amazon e de outras fontes. CloudTrail CloudWatch Os registros podem monitorar as informações nos arquivos de log e notificá-lo quando determinados limites forem atingidos. É possível também arquivar seus dados de log em armazenamento resiliente. Para obter mais informações, consulte o Guia do usuário do Amazon CloudWatch Logs.
- AWS CloudTrailcaptura API chamadas e eventos relacionados feitos por ou em nome de sua AWS conta e entrega os arquivos de log para um bucket do Amazon S3 que você especificar. Você pode identificar quais usuários e contas ligaram AWS, o endereço IP de origem a partir do qual as chamadas foram feitas e quando elas ocorreram. Para obter mais informações, consulte o Guia do usuário do AWS CloudTrail.

Monitorando as mensagens sociais do usuário AWS final com a Amazon CloudWatch

Você pode monitorar o AWS End User Messaging Social usando CloudWatch, que coleta dados brutos e os processa em métricas legíveis, quase em tempo real. Essas estatísticas são mantidas por 15 meses, de maneira que você possa acessar informações históricas e ter uma perspectiva melhor de como o aplicativo web ou o serviço está se saindo. Você também pode definir alarmes que observam determinados limites e enviam notificações ou realizam ações quando esses limites são atingidos. Para obter mais informações, consulte o Guia CloudWatch do usuário da Amazon.

Para o AWS End User Messaging Social, talvez você queira observar`WhatsAppMessageFeeCount`, assistir `WhatsAppConversationFeeCount` e acionar um alarme quando um limite de gastos for atingido.

> **Note**
>
> Antes de usar as CloudWatch métricas, você deve criar uma função de link de serviço.

As tabelas a seguir listam as métricas e dimensões que o AWS End User Messaging Social exporta para o `AWS/SocialMessaging` namespace.

Métrica	Unidade	Descrição
WhatsAppConversationFeeCount	Contagem	A contagem das taxas de WhatsApp conversação
WhatsAppMessageFeeCount	Contagem	A contagem das taxas de WhatsApp mensagens

Dimensão	Descrição
MessageFeeType	Os tipos de taxas válidas são Serviço, Marketing, Serviços Públicos e Autenticação
DestinationCountryCode	O ISO código de duas letras do país
WhatsAppPhoneNumberArn	O braço do número de telefone

Registrando API chamadas sociais de mensagens do usuário AWS final usando AWS CloudTrail

AWS O é integrado ao AWS CloudTrail, um serviço que fornece um registro das ações realizadas por um usuário, por um perfil ou por um serviço da no Systams AWS service (Serviço da AWS). CloudTrail captura todas as API chamadas para o AWS End User Messaging Social como eventos.

As chamadas capturadas incluem chamadas de código para as AWS API operações da API do console do AWS AppStream. Usando as informações coletadas pelo CloudTrail, é possível determinar a solicitação que foi feita ao, o endereço IP AWS no qual a solicitação foi feita, quando a solicitação foi feita, quando a solicitação foi feita, quando a solicitação foi feita, quando a solicitação foi feita, quando a solicitação foi feita e outros detalhes.

Cada entrada de log ou evento contém informações sobre quem gerou a solicitação. As informações de identidade ajudam a determinar:

- Se a solicitação foi feita com credenciais de usuário raiz ou credenciais de usuário.
- Se a solicitação foi feita em nome de um usuário do Centro de IAM Identidade do IAM.
- Se a solicitação foi feita com credenciais de segurança temporárias de um perfil ou de um usuário federado.
- Se a solicitação foi feita por outro AWS service (Serviço da AWS).

CloudTrail Criar uma trilha de Conta da AWS várias regiões é uma prática recomendada, pois você tem acesso automático ao Histórico de CloudTrail eventos. O Histórico de CloudTrail eventos fornece um registro visualizável, pesquisável, baixável e imutável dos últimos 90 dias de eventos de gerenciamento em uma. Região da AWS Para obter mais informações, consulte Trabalhando com o histórico de CloudTrail eventos no Guia AWS CloudTrail do usuário. Não há CloudTrail cobranças do Histórico de eventos.

Para obter um registro contínuo de eventos em sua Conta da AWS nos últimos 90 dias, consulte. CloudTrail

CloudTrail trilhas

Uma trilha permite que CloudTrail o CloudTrail entregue arquivos de log a um bucket do Amazon S3. As trilhas criadas usando o AWS Management Console são de várias regiões. Só é possível criar uma trilha de região única ou de várias regiões usando a AWS CLI. Criar uma trilha de várias regiões é uma prática recomendada, pois você captura atividades Regiões da AWS em todas as regiões da conta. Se você criar uma trilha de região única, poderá visualizar somente os eventos registrados na Região da AWS da trilha. Para obter mais informações sobre trilhas, consulte Criar uma trilha para a Conta da AWS e Criar uma trilha para uma organização no Guia do usuário do AWS CloudTrail .

Uma cópia dos seus eventos de gerenciamento em andamento pode ser entregue no console do Amazon S3 sem nenhum custo via CloudTrail com a criação CloudTrail de uma trilha. No entanto,

há cobranças de armazenamento do Amazon S3. Para obter mais informações sobre CloudTrail preços, consulte AWS CloudTrail Preços. Para receber informações sobre a definição de preço do Amazon S3, consulte Definição de preço do Amazon S3.

CloudTrail Armazenamentos de dados de eventos do Lake

CloudTrail O Lake permite que você execute consultas SQL baseadas em SQL em seus eventos. CloudTrail O Lake permite que você execute consultas baseadas em linhas para o JSON formato JSON. ORC ORCO ORC é um formato colunar de armazenamento otimizado para recuperação rápida de dados. Os eventos são agregados em armazenamentos de dados de eventos, que são coleções imutáveis de eventos baseados nos critérios selecionados com a aplicação de seletores de eventos avançados. Os seletores que você aplica a um armazenamento de dados de eventos controlam quais eventos persistem e estão disponíveis para você consultar. Para obter mais informações sobre o CloudTrail Lake, consulte Trabalhando com o AWS CloudTrail Lake no Guia AWS CloudTrail do Usuário.

CloudTrail Os armazenamentos de dados e consultas de eventos do Lake incorrem em cobranças. Ao criar um armazenamento de dados de eventos, você escolhe a opção de preço que deseja usar para ele. A opção de preço determina o custo para a ingestão e para o armazenamento de eventos, e o período de retenção padrão e máximo para o armazenamento de dados de eventos. Para obter mais informações sobre CloudTrail preços, consulte AWS CloudTrail Preços.

AWS Mensagens para o usuário final Eventos de dados sociais em CloudTrail

Os eventos de dados fornecem informações sobre as operações de recursos realizadas em um recurso (por exemplo, leitura ou gravação em um objeto do Amazon S3). Elas também são conhecidas como operações de plano de dados. Eventos de dados geralmente são atividades de alto volume. Por padrão, o CloudTrail CloudTrail não registra eventos de dados em log. O Histórico de CloudTrail eventos do CloudTrail não registra eventos de dados.

Há cobranças adicionais para eventos de dados. Para obter mais informações sobre CloudTrail preços, consulte AWS CloudTrail Preços.

Você pode registrar eventos de dados para os tipos de recursos sociais do AWS End User Messaging usando o CloudTrail console ou CloudTrail API as operações. AWS CLI Para obter mais informações sobre como registrar eventos de dados em log, consulte Registrar eventos de

dados com o AWS Management Console e Registrar eventos de dados com a AWS Command Line Interface no Guia do usuário do AWS CloudTrail .

A tabela a seguir lista o tipo AWS de recurso do Amazon S3 para o qual é possível registrar eventos de dados em log. A coluna Tipo de evento de dados (console) mostra o valor a ser escolhido na CloudTrail lista. A coluna do valor resources.type mostra o valor de resources.type que você especificaria ao `resources.type` configurar seletores de eventos avançados usando a ou as APIs do CloudTrail. AWS CLI CloudTrail APIs A CloudTrail coluna Dados APIs registrados mostra as API chamadas registradas CloudTrail para o tipo de recurso.

Tipo de evento de dados (console)	valor resources.type	Dados APIs registrados em CloudTrail
ID do número de telefone de mensagens sociais	`AWS::SocialMessaging::PhoneNumberId`	• DeleteWhatsAppMessageMedia • GetWhatsAppMessageMedia • PostWhatsAppMessageMedia • SendWhatsAppMessage

É possível configurar seletores de eventos avançados para filtrar os campos `eventName`, `readOnly` e `resources.ARN` para registrar em log somente os eventos que são importantes para você. Para obter mais informações sobre esses campos, consulte. AdvancedFieldSelectorna AWS CloudTrail APIReferência.

AWS Mensagens para o usuário final Eventos de gerenciamento social em CloudTrail

Os eventos de gerenciamento fornecem informações sobre operações de gerenciamento executadas em recursos na sua Conta da AWS. Elas também são conhecidas como operações de plano de controle. Por padrão, há CloudTrail cobranças de gerenciamento em log.

AWS O Amazon CloudTrail AWS registra em log todas as operações do ambiente de gerenciamento como eventos de gerenciamento. Para obter uma lista das operações do plano de controle do AWS End User Messaging Social nas quais o AWS End User Messaging Social se conecta CloudTrail, consulte a APIReferência Social do AWS End User Messaging.

AWS Mensagens para usuários finais: exemplos de eventos sociais

Um evento representa uma única solicitação de qualquer origem e inclui informações sobre a API operação solicitada, a data e a hora em que ocorreram, os parâmetros de solicitação etc. CloudTrail Os arquivos de log do Lake não são um rastreamento de pilha ordenada de API chamadas de API pública. Dessa forma, eles não são exibidos em uma ordem específica.

O exemplo a seguir mostra uma entrada CloudTrail de log do que demonstra a operação.


```
{
        "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"
        }
    }
```


Para obter informações sobre o conteúdo do CloudTrail registro, consulte o conteúdo do CloudTrail registro no Guia AWS CloudTrail do usuário.

Práticas recomendadas para mensagens sociais para usuários AWS finais

Esta seção descreve várias práticas recomendadas que podem ajudar você a melhorar o engajamento do cliente e evitar a suspensão da conta. No entanto, observe que esta seção não contém orientação jurídica. Sempre consulte seu advogado para obter orientação jurídica.

Para ver a lista mais recente das WhatsApp melhores práticas, consulte a Política de mensagens WhatsApp comerciais.

Tópicos

- Up-to-date perfil de negócios
- Obter permissão
- Conteúdo de mensagem proibido
- Fazer auditoria em suas listas de clientes
- Ajustar seu envio com base no envolvimento
- Enviar em momentos adequados

Up-to-date perfil de negócios

Mantenha um perfil up-to-date WhatsApp comercial preciso que inclua informações de contato do suporte ao cliente, como endereço de e-mail, endereço do site ou número de telefone. Certifique-se de que as informações fornecidas sejam verdadeiras e não deturpem ou se passem por outra empresa.

Obter permissão

Nunca envie mensagens a destinatários que não tenham solicitado explicitamente o recebimento dos tipos específicos de mensagens que você planeja enviar. Mantenha as seguintes informações de aceitação:

- O processo de aceitação deve informar claramente à pessoa que ela está consentindo em receber mensagens ou ligações da sua empresa. WhatsApp Você deve declarar explicitamente o nome da sua empresa.

- Você é o único responsável por determinar o método de obtenção do consentimento opcional. Certifique-se de que o processo de aceitação esteja em conformidade com todas as leis aplicáveis que regem suas comunicações. Forneça todos os avisos necessários e obtenha todas as permissões necessárias de acordo com as leis relevantes.

Para obter mais informações sobre os requisitos de WhatsApp aceitação, consulte Obter aceitação para WhatsApp

Se os destinatários puderem se inscrever para receber suas mensagens usando um formulário on-line, evite que scripts automatizados inscrevam pessoas sem o conhecimento delas. Limite também o número de vezes que um usuário pode enviar um número de telefone em uma única sessão.

Respeite todas as solicitações feitas por uma pessoa, ativada ou desativada WhatsApp, para bloquear, interromper ou optar por não receber comunicações, incluindo a remoção dessa pessoa da sua lista de contatos.

Mantenha registros que incluem a data, a hora e a origem de cada solicitação de inclusão e confirmação de inscrição. Isso também pode ajudá-lo a realizar auditorias de rotina da sua lista de clientes.

Conteúdo de mensagem proibido

⚠ Important

Trabalhando com Meta/ WhatsApp

- Seu uso da Solução WhatsApp Empresarial está sujeito aos termos e condições dos Termos de Serviço WhatsApp Empresariais, dos Termos da Solução WhatsApp Empresarial, da Política de Mensagens WhatsApp Comerciais, das Diretrizes de WhatsApp Mensagens e de todos os outros termos, políticas ou diretrizes incorporados a eles por referência (pois cada um pode ser atualizado periodicamente).
- A Meta ou WhatsApp pode, a qualquer momento, proibir seu uso da Solução WhatsApp Empresarial.
- Em conexão com o uso da Solução WhatsApp Empresarial, você não enviará nenhum conteúdo, informação ou dado que esteja sujeito a salvaguardas ou limitações na distribuição de acordo com as leis ou regulamentos aplicáveis.

Se você violar a WhatsApp política, sua conta poderá ser impedida de enviar mensagens por um período de tempo, bloqueada até que você registre uma apelação ou bloqueada permanentemente. A Meta informará se alguma de suas contas ou ativos violou a política, por e-mail e pelo gerente de WhatsApp negócios. Todos os apelos devem ser feitos à Meta. Para ver uma violação de política ou registrar uma apelação na Meta, consulte Exibir detalhes da violação de política da sua conta WhatsApp comercial na Central de Ajuda da Meta Business. Para obter a lista mais recente de conteúdo de mensagens proibidas, consulte a Política de mensagens WhatsApp comerciais.

A seguir estão as categorias de conteúdo proibidas para todos os tipos de mensagens em todo o mundo. Ao enviar uma mensagem com WhatsApp, siga estas diretrizes:

Categoria	Exemplos
Jogos de aposta	• Cassinos • Sorteios • Aplicativos/sites
Serviços financeiros de alto risco	• Empréstimos consignados • Empréstimos de curto prazo com juros elevados • Autoempréstimos • Empréstimos hipotecários • Empréstimos estudantis • Cobrança de dívidas • Alertas de ações • Criptomoedas
Perdão de dívidas	• Consolidação de dívidas • Redução des dívida • Programas de restauração de crédito
Get-rich-quick esquemas	• Work-from-home programas • Oportunidades de investimento de risco • Esquemas de pirâmide ou de marketing multinível

Categoria	Exemplos
Substâncias ilegais	• Cannabis/CBD
Phishing/smishing	• Tenta fazer com que os usuários revelem informações pessoais ou informações de login em sites.
S.H.A.F.T.	• Sexo • Ódio • Álcool • Armas de fogo • Tabaco/Cigarro eletrônico
Geração de leads de terceiros	• Empresas que compram, vendem ou compartilham informações de consumidores

Fazer auditoria em suas listas de clientes

Se você enviar WhatsApp mensagens recorrentes, audite suas listas de clientes regularmente. A auditoria de suas listas de clientes ajuda a garantir que os únicos clientes que recebem suas mensagens sejam aqueles que desejam recebê-las.

Ao fazer uma auditoria em sua lista, envie a cada cliente incluído uma mensagem que lembre a ele que está inscrito e ofereça informações sobre o cancelamento da inscrição.

Ajustar seu envio com base no envolvimento

As prioridades de seus clientes podem mudar ao longo do tempo. Se os clientes não acham mais suas mensagens úteis, eles podem querer cancelar a inscrição para suas mensagens ou até mesmo informar suas mensagens como não solicitadas. Por esses motivos, é importante que você ajuste suas práticas de envio com base no envolvimento do cliente.

Você precisa ajustar a frequência de suas mensagens para clientes que raramente interagem com elas. Por exemplo, se você envia mensagens semanais para clientes envolvidos, pode criar uma compilação mensal separada para os clientes com menos envolvimento.

Por fim, remova das suas listas de clientes aqueles que não têm nenhum envolvimento. Essa etapa impede que os clientes fiquem frustrados com suas mensagens. Isso também gera economia e ajuda a proteger sua reputação como remetente.

Enviar em momentos adequados

Envie mensagens durante o horário comercial normal. Se você enviar mensagens na hora do jantar ou no meio da noite, há uma boa chance de seus clientes cancelarem a assinatura de suas listas para evitar serem incomodados. Talvez você queira evitar o envio de WhatsApp mensagens quando seus clientes não conseguem responder imediatamente.

Segurança nas mensagens sociais do usuário AWS final

A segurança na nuvem AWS é a maior prioridade. Como AWS cliente, você se beneficia de data centers e arquiteturas de rede criados para atender aos requisitos das organizações mais sensíveis à segurança.

A segurança é uma responsabilidade compartilhada entre você AWS e você. O modelo de responsabilidade compartilhada descreve isso como segurança da nuvem e segurança na nuvem:

- Segurança da nuvem — AWS é responsável por proteger a infraestrutura que executa AWS os serviços no Nuvem AWS. AWS também fornece serviços que você pode usar com segurança. Auditores terceirizados testam e verificam regularmente a eficácia de nossa segurança como parte dos Programas de Conformidade Programas de AWS de . Para saber mais sobre os programas de conformidade que se aplicam ao AWS End User Messaging Social, consulte AWS Serviços no escopo do programa de conformidade AWS .
- Segurança na nuvem — Sua responsabilidade é determinada pelo AWS serviço que você usa. Você também é responsável por outros fatores, incluindo a confidencialidade de seus dados, os requisitos da empresa e as leis e regulamentos aplicáveis.

Esta documentação ajuda você a entender como aplicar o modelo de responsabilidade compartilhada ao usar o AWS End User Messaging Social. Os tópicos a seguir mostram como configurar o AWS End User Messaging Social para atender aos seus objetivos de segurança e conformidade. Você também aprenderá a usar outros AWS serviços que ajudam a monitorar e proteger seus recursos sociais de mensagens para usuários AWS finais.

Tópicos

- Proteção de dados nas redes sociais de mensagens do usuário AWS final
- Gerenciamento de identidade e acesso para mensagens sociais de usuários AWS finais
- Validação de conformidade para mensagens sociais de usuário AWS final
- Resiliência nas mensagens AWS sociais do usuário final
- Segurança da infraestrutura nas redes sociais de mensagens do usuário AWS final
- Prevenção contra o ataque do “substituto confuso” em todos os serviços
- Práticas recomendadas de segurança
- Usando funções vinculadas a serviços para mensagens sociais de usuário AWS final

Proteção de dados nas redes sociais de mensagens do usuário AWS final

O modelo de responsabilidade AWS compartilhada se aplica à proteção de dados no AWS End User Messaging Social. Conforme descrito neste modelo, AWS é responsável por proteger a infraestrutura global que executa todos os Nuvem AWS. Você é responsável por manter o controle sobre o conteúdo hospedado nessa infraestrutura. Você também é responsável pelas tarefas de configuração e gerenciamento de segurança dos Serviços da AWS que usa. Para obter mais informações sobre a privacidade de dados, consulte as Data Privacy FAQ. Para obter mais informações sobre a proteção de dados na Europa, consulte a postagem do blog AWS Shared Responsibility Model and RGPD no Blog de segurança da AWS .

Para fins de proteção de dados, recomendamos que você proteja Conta da AWS as credenciais e configure usuários individuais com AWS IAM Identity Center ou AWS Identity and Access Management (IAM). Dessa maneira, cada usuário receberá apenas as permissões necessárias para cumprir suas obrigações de trabalho. Recomendamos também que você proteja seus dados das seguintes formas:

- Use uma autenticação multifator (MFA) com cada conta.
- Use SSL/TLS para se comunicar com os recursos. AWS Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Configure a API e o registro de atividades do usuário com AWS CloudTrail. Para obter informações sobre o uso de CloudTrail trilhas para capturar AWS atividades, consulte Como trabalhar com CloudTrail trilhas no Guia AWS CloudTrail do usuário.
- Use soluções de AWS criptografia, juntamente com todos os controles de segurança padrão Serviços da AWS.
- Use serviços gerenciados de segurança avançada, como o Amazon Macie, que ajuda a localizar e proteger dados sigilosos armazenados no Amazon S3.
- Se você precisar de módulos criptográficos validados pelo FIPS 140-3 ao acessar AWS por meio de uma interface de linha de comando ou de uma API, use um endpoint FIPS. Para obter mais informações sobre os endpoints FIPS disponíveis, consulte Federal Information Processing Standard (FIPS) 140-3.

É altamente recomendável que nunca sejam colocadas informações confidenciais ou sigilosas, como endereços de e-mail de clientes, em tags ou campos de formato livre, como um campo Nome.

Isso inclui quando você trabalha com o AWS End User Messaging Social ou outro Serviços da AWS usando o console AWS CLI, a API ou AWS SDKs. Quaisquer dados inseridos em tags ou em campos de texto de formato livre usados para nomes podem ser usados para logs de faturamento ou de diagnóstico. Se você fornecer um URL para um servidor externo, é fortemente recomendável que não sejam incluídas informações de credenciais no URL para validar a solicitação nesse servidor.

> **Important**
>
> WhatsApp usa o protocolo Signal para comunicações seguras. No entanto, como o AWS End User Messaging Social é de terceiros, WhatsApp não considera essas mensagens end-to-end criptografadas. Para obter mais informações sobre proteção WhatsApp de dados, consulte o whitepaper Visão geral sobre privacidade e segurança de dados e WhatsApp criptografia.

Criptografia de dados

AWS Mensagens para o usuário final Os dados sociais são criptografados em trânsito e em repouso dentro dos AWS limites. Quando você envia dados para o AWS End User Messaging Social, ele criptografa os dados à medida que são recebidos e os armazena. Quando você recupera dados do AWS End User Messaging Social, ele transmite os dados para você usando os protocolos de segurança atuais.

Criptografia em repouso

AWS O End User Messaging Social criptografa todos os dados que ele armazena para você dentro do AWS limite. Isso inclui dados de configuração, dados de registro e quaisquer dados que você adicionar ao AWS End User Messaging Social. Para criptografar seus dados, o AWS End User Messaging Social usa chaves internas AWS Key Management Service (AWS KMS) que o serviço possui e mantém em seu nome. Para obter mais informações sobre o AWS KMS, consulte o Guia do desenvolvedor do AWS Key Management Service.

Criptografia em trânsito

AWS O End User Messaging Social usa HTTPS e Transport Layer Security (TLS) 1.2 para se comunicar com seus clientes, aplicativos e Meta. Para se comunicar com outros AWS serviços, o AWS End User Messaging Social usa HTTPS e TLS 1.2. Além disso, quando você cria e gerencia recursos sociais de mensagens de usuário AWS final usando o console, um AWS SDK ou o. AWS Command Line Interface, todas as comunicações são protegidas usando HTTPS e TLS 1.2.

Gerenciamento de chaves

Para criptografar seus dados, o AWS End User Messaging Social usa AWS KMS chaves internas que o serviço possui e mantém em seu nome. Nós mudamos essas chaves regularmente. Você não pode provisionar e usar suas próprias chaves AWS KMS ou outras chaves para criptografar dados que você armazena no AWS End User Messaging Social.

Privacidade do tráfego entre redes

A privacidade do tráfego entre redes se refere à proteção de conexões e tráfego entre o AWS End User Messaging Social e seus clientes e aplicativos locais, e entre o AWS End User Messaging Social e outros AWS recursos no mesmo. Região da AWS Os recursos e práticas a seguir podem ajudá-lo a proteger a privacidade do tráfego entre redes sociais para o AWS End User Messaging Social.

Tráfego entre clientes e aplicativos sociais de mensagens de usuário AWS final e locais

Para estabelecer uma conexão privada entre AWS End User Messaging Social e clientes e aplicativos em sua rede local, você pode usar AWS Direct Connect. Isso permite vincular a rede a um local do AWS Direct Connect usando um cabo Ethernet de fibra ótica padrão. Uma extremidade do cabo é conectada ao roteador. A outra extremidade está conectada a um AWS Direct Connect roteador. Para obter mais informações, consulte O que é o AWS Direct Connect? no Guia do usuário do AWS Direct Connect .

Para ajudar a proteger o acesso ao AWS End User Messaging Social por meio do Published APIs, recomendamos que você cumpra os requisitos do AWS End User Messaging Social para chamadas de API. AWS O End User Messaging Social exige que os clientes usem o Transport Layer Security (TLS) 1.2 ou posterior. Os clientes também devem oferecer suporte a pacotes de criptografia com sigilo de encaminhamento perfeito (PFS), como Ephemeral Diffie-Hellman (DHE) ou Ephemeral Elliptic Curve Diffie-Hellman (ECDHE). A maioria dos sistemas modernos como Java 7 e versões posteriores oferece suporte a esses modos.

Além disso, as solicitações devem ser assinadas usando um ID de chave de acesso e uma chave de acesso secreta associada a um principal AWS Identity and Access Management (IAM) da sua AWS conta. Como alternativa, você pode usar o AWS Security Token Service (AWS STS) para gerar credenciais de segurança temporárias para assinar solicitações.

Gerenciamento de identidade e acesso para mensagens sociais de usuários AWS finais

AWS Identity and Access Management (IAM) é uma ferramenta AWS service (Serviço da AWS) que ajuda o administrador a controlar com segurança o acesso aos AWS recursos. Os administradores do IAM controlam quem pode ser autenticado (conectado) e autorizado (tem permissões) para usar os recursos sociais de mensagens do usuário AWS final. O IAM é um AWS service (Serviço da AWS) que você pode usar sem custo adicional.

Tópicos

- Público
- Autenticar com identidades
- Gerenciar o acesso usando políticas
- Como o AWS End User Messaging Social funciona com o IAM
- Exemplos de políticas baseadas em identidade para redes sociais de mensagens de usuário AWS final
- AWS políticas gerenciadas para redes sociais de mensagens de usuário AWS final
- Solução de problemas de mensagens de usuário AWS final: identidade social e acesso

Público

A forma como você usa o AWS Identity and Access Management (IAM) difere, dependendo do trabalho que você faz no AWS End User Messaging Social.

Usuário do serviço — Se você usa o serviço social AWS End User Messaging para fazer seu trabalho, seu administrador fornecerá as credenciais e as permissões de que você precisa. À medida que você usa mais recursos sociais de mensagens de usuário AWS final para fazer seu trabalho, talvez precise de permissões adicionais. Compreenda como o acesso é gerenciado pode ajudar a solicitar as permissões corretas ao administrador. Se você não conseguir acessar um recurso no AWS End User Messaging Social, consulteSolução de problemas de mensagens de usuário AWS final: identidade social e acesso.

Administrador de serviços — Se você é responsável pelos recursos sociais de mensagens do usuário AWS final em sua empresa, provavelmente tem acesso total ao sistema social de mensagens do usuário AWS final. É seu trabalho determinar quais recursos e recursos sociais de

mensagens de usuário AWS final seus usuários do serviço devem acessar. Envie as solicitações ao administrador do IAM para alterar as permissões dos usuários de serviço. Revise as informações nesta página para compreender os conceitos básicos do IAM. Para saber mais sobre como sua empresa pode usar o IAM com o AWS End User Messaging Social, consulteComo o AWS End User Messaging Social funciona com o IAM.

Administrador do IAM — Se você for administrador do IAM, talvez queira saber detalhes sobre como criar políticas para gerenciar o acesso ao AWS End User Messaging Social. Para ver exemplos de políticas baseadas em identidade social de mensagens de usuário AWS final que você pode usar no IAM, consulte. Exemplos de políticas baseadas em identidade para redes sociais de mensagens de usuário AWS final

Autenticar com identidades

A autenticação é como você faz login AWS usando suas credenciais de identidade. Você deve estar autenticado (conectado AWS) como o Usuário raiz da conta da AWS, como usuário do IAM ou assumindo uma função do IAM.

Você pode entrar AWS como uma identidade federada usando credenciais fornecidas por meio de uma fonte de identidade. AWS IAM Identity Center Usuários (IAM Identity Center), a autenticação de login único da sua empresa e suas credenciais do Google ou do Facebook são exemplos de identidades federadas. Quando você faz login como identidade federada, o administrador já configurou anteriormente a federação de identidades usando perfis do IAM. Ao acessar AWS usando a federação, você está assumindo indiretamente uma função.

Dependendo do tipo de usuário que você é, você pode entrar no AWS Management Console ou no portal de AWS acesso. Para obter mais informações sobre como fazer login em AWS, consulte Como fazer login Conta da AWS no Guia do Início de Sessão da AWS usuário.

Se você acessar AWS programaticamente, AWS fornece um kit de desenvolvimento de software (SDK) e uma interface de linha de comando (CLI) para assinar criptograficamente suas solicitações usando suas credenciais. Se você não usa AWS ferramentas, você mesmo deve assinar as solicitações. Para obter mais informações sobre como usar o método recomendado para designar solicitações por conta própria, consulte Versão 4 do AWS Signature para solicitações de API no Guia do usuário do IAM.

Independente do método de autenticação usado, também pode ser necessário fornecer informações adicionais de segurança. Por exemplo, AWS recomenda que você use a autenticação multifator (MFA) para aumentar a segurança da sua conta. Para saber mais, consulte Autenticação multifator

no Guia do usuário do AWS IAM Identity Center e Usar a autenticação multifator da AWS no IAM no Guia do usuário do IAM.

Conta da AWS usuário root

Ao criar uma Conta da AWS, você começa com uma identidade de login que tem acesso completo a todos Serviços da AWS os recursos da conta. Essa identidade é chamada de usuário Conta da AWS raiz e é acessada fazendo login com o endereço de e-mail e a senha que você usou para criar a conta. É altamente recomendável não usar o usuário-raiz para tarefas diárias. Proteja as credenciais do usuário-raiz e use-as para executar as tarefas que somente ele puder executar. Para obter a lista completa das tarefas que exigem login como usuário-raiz, consulte Tarefas que exigem credenciais de usuário-raiz no Guia do Usuário do IAM.

Identidade federada

Como prática recomendada, exija que usuários humanos, incluindo usuários que precisam de acesso de administrador, usem a federação com um provedor de identidade para acessar Serviços da AWS usando credenciais temporárias.

Uma identidade federada é um usuário do seu diretório de usuários corporativo, de um provedor de identidade da web AWS Directory Service, do diretório do Identity Center ou de qualquer usuário que acesse usando credenciais fornecidas Serviços da AWS por meio de uma fonte de identidade. Quando as identidades federadas são acessadas Contas da AWS, elas assumem funções, e as funções fornecem credenciais temporárias.

Para o gerenciamento de acesso centralizado, é recomendável usar o AWS IAM Identity Center. Você pode criar usuários e grupos no IAM Identity Center ou pode se conectar e sincronizar com um conjunto de usuários e grupos em sua própria fonte de identidade para uso em todos os seus Contas da AWS aplicativos. Para obter mais informações sobre o Centro de Identidade do IAM, consulte O que é o Centro de Identidade do IAM? no Guia do Usuário do AWS IAM Identity Center .

Usuários e grupos do IAM

Um usuário do IAM é uma identidade dentro da sua Conta da AWS que tem permissões específicas para uma única pessoa ou aplicativo. Sempre que possível, é recomendável contar com credenciais temporárias em vez de criar usuários do IAM com credenciais de longo prazo, como senhas e chaves de acesso. No entanto, se você tiver casos de uso específicos que exijam credenciais de longo prazo com usuários do IAM, é recomendável alternar as chaves de acesso. Para obter mais informações, consulte Alternar as chaves de acesso regularmente para casos de uso que exijam credenciais de longo prazo no Guia do Usuário do IAM.

Um grupo do IAM é uma identidade que especifica uma coleção de usuários do IAM. Não é possível fazer login como um grupo. É possível usar grupos para especificar permissões para vários usuários de uma vez. Os grupos facilitam o gerenciamento de permissões para grandes conjuntos de usuários. Por exemplo, você pode ter um grupo chamado IAMAdminse conceder a esse grupo permissões para administrar recursos do IAM.

Usuários são diferentes de perfis. Um usuário é exclusivamente associado a uma pessoa ou a uma aplicação, mas um perfil pode ser assumido por qualquer pessoa que precisar dele. Os usuários têm credenciais permanentes de longo prazo, mas os perfis fornecem credenciais temporárias. Para saber mais, consulte Casos de uso para usuários do IAM no Guia do usuário do IAM.

Perfis do IAM

Uma função do IAM é uma identidade dentro da sua Conta da AWS que tem permissões específicas. Ele é semelhante a um usuário do IAM, mas não está associado a uma pessoa específica. Para assumir temporariamente uma função do IAM no AWS Management Console, você pode alternar de um usuário para uma função do IAM (console). Você pode assumir uma função chamando uma operação de AWS API AWS CLI ou usando uma URL personalizada. Para obter mais informações sobre métodos para usar perfis, consulte Métodos para assumir um perfil no Guia do usuário do IAM.

Perfis do IAM com credenciais temporárias são úteis nas seguintes situações:

- Acesso de usuário federado: para atribuir permissões a identidades federadas, é possível criar um perfil e definir permissões para ele. Quando uma identidade federada é autenticada, essa identidade é associada ao perfil e recebe as permissões definidas por ele. Para ter mais informações sobre perfis para federação, consulte Criar um perfil para um provedor de identidade de terceiros (federação) no Guia do usuário do IAM. Se usar o Centro de Identidade do IAM, configure um conjunto de permissões. Para controlar o que suas identidades podem acessar após a autenticação, o Centro de Identidade do IAM correlaciona o conjunto de permissões a um perfil no IAM. Para obter informações sobre conjuntos de permissões, consulte Conjuntos de Permissões no Guia do Usuário do AWS IAM Identity Center .
- Permissões temporárias para usuários do IAM: um usuário ou um perfil do IAM pode presumir um perfil do IAM para obter temporariamente permissões diferentes para uma tarefa específica.
- Acesso entre contas: é possível usar um perfil do IAM para permitir que alguém (uma entidade principal confiável) em outra conta acesse recursos em sua conta. Os perfis são a principal forma de conceder acesso entre contas. No entanto, com alguns Serviços da AWS, você pode anexar uma política diretamente a um recurso (em vez de usar uma função como proxy). Para conhecer a

diferença entre perfis e políticas baseadas em recurso para acesso entre contas, consulte Acesso a recursos entre contas no IAM no Guia do usuário do IAM.

- Acesso entre serviços — Alguns Serviços da AWS usam recursos em outros Serviços da AWS. Por exemplo, quando você faz uma chamada em um serviço, é comum que esse serviço execute aplicativos na Amazon EC2 ou armazene objetos no Amazon S3. Um serviço pode fazer isso usando as permissões da entidade principal da chamada, usando um perfil de serviço ou um perfil vinculado ao serviço.
  - Sessões de acesso direto (FAS) — Quando você usa um usuário ou uma função do IAM para realizar ações AWS, você é considerado principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. O FAS usa as permissões do diretor chamando um AWS service (Serviço da AWS), combinadas com a solicitação AWS service (Serviço da AWS) para fazer solicitações aos serviços posteriores. As solicitações do FAS são feitas somente quando um serviço recebe uma solicitação que requer interações com outros Serviços da AWS ou com recursos para ser concluída. Nesse caso, você precisa ter permissões para executar ambas as ações. Para obter detalhes da política ao fazer solicitações de FAS, consulte Sessões de acesso direto.
  - Perfil de serviço: um perfil de serviço é um perfil do IAM que um serviço assume para executar ações em seu nome. Um administrador do IAM pode criar, modificar e excluir um perfil de serviço do IAM. Para obter mais informações, consulte Criar um perfil para delegar permissões a um AWS service (Serviço da AWS) no Guia do Usuário do IAM.
  - Função vinculada ao serviço — Uma função vinculada ao serviço é um tipo de função de serviço vinculada a um. AWS service (Serviço da AWS) O serviço pode presumir o perfil de executar uma ação em seu nome. As funções vinculadas ao serviço aparecem em você Conta da AWS e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não editar as permissões para perfis vinculados ao serviço.
- Aplicativos em execução na Amazon EC2 — Você pode usar uma função do IAM para gerenciar credenciais temporárias para aplicativos que estão sendo executados em uma EC2 instância e fazendo solicitações AWS CLI de AWS API. Isso é preferível a armazenar chaves de acesso na EC2 instância. Para atribuir uma AWS função a uma EC2 instância e disponibilizá-la para todos os aplicativos, você cria um perfil de instância anexado à instância. Um perfil de instância contém a função e permite que programas em execução na EC2 instância recebam credenciais temporárias. Para obter mais informações, consulte Usar uma função do IAM para conceder permissões a aplicativos executados em EC2 instâncias da Amazon no Guia do usuário do IAM.

Gerenciar o acesso usando políticas

Você controla o acesso AWS criando políticas e anexando-as a AWS identidades ou recursos. Uma política é um objeto AWS que, quando associada a uma identidade ou recurso, define suas permissões. AWS avalia essas políticas quando um principal (usuário, usuário raiz ou sessão de função) faz uma solicitação. As permissões nas políticas determinam se a solicitação será permitida ou negada. A maioria das políticas é armazenada AWS como documentos JSON. Para obter mais informações sobre a estrutura e o conteúdo de documentos de políticas JSON, consulte Visão geral das políticas JSON no Guia do usuário do IAM.

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

Por padrão, usuários e perfis não têm permissões. Para conceder permissão aos usuários para executar ações nos recursos que eles precisam, um administrador do IAM pode criar políticas do IAM. O administrador pode então adicionar as políticas do IAM aos perfis e os usuários podem assumir os perfis.

As políticas do IAM definem permissões para uma ação independentemente do método usado para executar a operação. Por exemplo, suponha que você tenha uma política que permite a ação `iam:GetRole`. Um usuário com essa política pode obter informações de função da AWS Management Console AWS CLI, da ou da AWS API.

Políticas baseadas em identidade

As políticas baseadas em identidade são documentos de políticas de permissões JSON que você pode anexar a uma identidade, como usuário, grupo de usuários ou perfil do IAM. Essas políticas controlam quais ações os usuários e perfis podem realizar, em quais recursos e em que condições. Para saber como criar uma política baseada em identidade, consulte Definir permissões personalizadas do IAM com as políticas gerenciadas pelo cliente no Guia do Usuário do IAM.

As políticas baseadas em identidade podem ser categorizadas como políticas em linha ou políticas gerenciadas. As políticas em linha são anexadas diretamente a um único usuário, grupo ou perfil. As políticas gerenciadas são políticas autônomas que você pode associar a vários usuários, grupos e funções em seu Conta da AWS. As políticas AWS gerenciadas incluem políticas gerenciadas e políticas gerenciadas pelo cliente. Para saber como escolher entre uma política gerenciada ou uma política em linha, consulte Escolher entre políticas gerenciadas e políticas em linha no Guia do usuário do IAM.

Políticas baseadas em recursos

Políticas baseadas em recursos são documentos de políticas JSON que você anexa a um recurso. São exemplos de políticas baseadas em recursos as políticas de confiança de perfil do IAM e as políticas de bucket do Amazon S3. Em serviços compatíveis com políticas baseadas em recursos, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. Para o atributo ao qual a política está anexada, a política define quais ações uma entidade principal especificado pode executar nesse atributo e em que condições. Você deve especificar uma entidade principal em uma política baseada em recursos. Os diretores podem incluir contas, usuários, funções, usuários federados ou. Serviços da AWS

Políticas baseadas em recursos são políticas em linha localizadas nesse serviço. Você não pode usar políticas AWS gerenciadas do IAM em uma política baseada em recursos.

Listas de controle de acesso (ACLs)

As listas de controle de acesso (ACLs) controlam quais diretores (membros da conta, usuários ou funções) têm permissões para acessar um recurso. ACLs são semelhantes às políticas baseadas em recursos, embora não usem o formato de documento de política JSON.

O Amazon S3 e o AWS WAF Amazon VPC são exemplos de serviços que oferecem suporte. ACLs Para saber mais ACLs, consulte a visão geral da lista de controle de acesso (ACL) no Guia do desenvolvedor do Amazon Simple Storage Service.

Outros tipos de política

AWS oferece suporte a tipos de políticas adicionais menos comuns. Esses tipos de política podem definir o máximo de permissões concedidas a você pelos tipos de política mais comuns.

- Limites de permissões: um limite de permissões é um recurso avançado no qual você define o máximo de permissões que uma política baseada em identidade pode conceder a uma entidade do IAM (usuário ou perfil do IAM). É possível definir um limite de permissões para uma entidade. As permissões resultantes são a interseção das políticas baseadas em identidade de uma entidade com seus limites de permissões. As políticas baseadas em recurso que especificam o usuário ou o perfil no campo `Principal` não são limitadas pelo limite de permissões. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações sobre limites de permissões, consulte Limites de permissões para identidades do IAM no Guia do usuário do IAM.

- Políticas de controle de serviço (SCPs) — SCPs são políticas JSON que especificam as permissões máximas para uma organização ou unidade organizacional (OU) em AWS Organizations. AWS Organizations é um serviço para agrupar e gerenciar centralmente vários Contas da AWS que sua empresa possui. Se você habilitar todos os recursos em uma organização, poderá aplicar políticas de controle de serviço (SCPs) a qualquer uma ou a todas as suas contas. O SCP limita as permissões para entidades nas contas dos membros, incluindo cada uma Usuário raiz da conta da AWS. Para obter mais informações sobre Organizations e SCPs, consulte Políticas de controle de serviços no Guia AWS Organizations do Usuário.
- Políticas de controle de recursos (RCPs) — RCPs são políticas JSON que você pode usar para definir o máximo de permissões disponíveis para recursos em suas contas sem atualizar as políticas do IAM anexadas a cada recurso que você possui. O RCP limita as permissões para recursos nas contas dos membros e pode afetar as permissões efetivas para identidades, incluindo a Usuário raiz da conta da AWS, independentemente de pertencerem à sua organização. Para obter mais informações sobre Organizations e RCPs, incluindo uma lista Serviços da AWS desse suporte RCPs, consulte Políticas de controle de recursos (RCPs) no Guia AWS Organizations do usuário.
- Políticas de sessão: são políticas avançadas que você transmite como um parâmetro quando cria de forma programática uma sessão temporária para um perfil ou um usuário federado. As permissões da sessão resultante são a interseção das políticas baseadas em identidade do usuário ou do perfil e das políticas de sessão. As permissões também podem ser provenientes de uma política baseada em recursos. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações, consulte Políticas de sessão no Guia do usuário do IAM.

Vários tipos de política

Quando vários tipos de política são aplicáveis a uma solicitação, é mais complicado compreender as permissões resultantes. Para saber como AWS determinar se uma solicitação deve ser permitida quando vários tipos de políticas estão envolvidos, consulte Lógica de avaliação de políticas no Guia do usuário do IAM.

Como o AWS End User Messaging Social funciona com o IAM

Antes de usar o IAM para gerenciar o acesso ao AWS End User Messaging Social, saiba quais recursos do IAM estão disponíveis para uso com o AWS End User Messaging Social.

Recursos do IAM que você pode usar com o AWS End User Messaging Social

Atributo do IAM	AWS Suporte social de mensagens para o usuário final
Políticas baseadas em identidade	Sim
Políticas baseadas em recurso	Não
Ações de políticas	Sim
Recursos de políticas	Sim
Chaves de condição de políticas	Sim
ACLs	Não
ABAC (tags em políticas)	Parcial
Credenciais temporárias	Sim
Permissões de entidade principal	Sim
Perfis de serviço	Sim
Perfis vinculados a serviço	Sim

Para ter uma visão de alto nível de como o AWS End User Messaging Social e outros AWS serviços funcionam com a maioria dos recursos do IAM, consulte AWS os serviços que funcionam com o IAM no Guia do usuário do IAM.

Políticas baseadas em identidade para mensagens sociais de usuários AWS finais

Compatível com políticas baseadas em identidade: sim

As políticas baseadas em identidade são documentos de políticas de permissões JSON que você pode anexar a uma identidade, como usuário do IAM, grupo de usuários ou perfil. Essas políticas controlam quais ações os usuários e perfis podem realizar, em quais recursos e em que condições. Para saber como criar uma política baseada em identidade, consulte Definir permissões personalizadas do IAM com as políticas gerenciadas pelo cliente no Guia do Usuário do IAM.

Com as políticas baseadas em identidade do IAM, é possível especificar ações e recursos permitidos ou negados, assim como as condições sob as quais as ações são permitidas ou negadas. Você não pode especificar a entidade principal em uma política baseada em identidade porque ela se aplica ao usuário ou perfil ao qual ela está anexada. Para saber mais sobre todos os elementos que podem ser usados em uma política JSON, consulte Referência de elemento de política JSON do IAM no Guia do usuário do IAM.

Exemplos de políticas baseadas em identidade para redes sociais de mensagens de usuário AWS final

Para ver exemplos de políticas baseadas em identidade social para mensagens de usuário AWS final, consulte. Exemplos de políticas baseadas em identidade para redes sociais de mensagens de usuário AWS final

Políticas baseadas em recursos no AWS End User Messaging Social

Compatibilidade com políticas baseadas em recursos: não

Políticas baseadas em recursos são documentos de políticas JSON que você anexa a um recurso. São exemplos de políticas baseadas em recursos as políticas de confiança de perfil do IAM e as políticas de bucket do Amazon S3. Em serviços compatíveis com políticas baseadas em recursos, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. Para o atributo ao qual a política está anexada, a política define quais ações uma entidade principal especificado pode executar nesse atributo e em que condições. Você deve especificar uma entidade principal em uma política baseada em recursos. Os diretores podem incluir contas, usuários, funções, usuários federados ou. Serviços da AWS

Para permitir o acesso entre contas, você pode especificar uma conta inteira ou as entidades do IAM em outra conta como a entidade principal em uma política baseada em recursos. Adicionar uma entidade principal entre contas à política baseada em recurso é apenas metade da tarefa de estabelecimento da relação de confiança. Quando o principal e o recurso são diferentes Contas da AWS, um administrador do IAM na conta confiável também deve conceder permissão à entidade principal (usuário ou função) para acessar o recurso. Eles concedem permissão ao anexar uma política baseada em identidade para a entidade. No entanto, se uma política baseada em recurso conceder acesso a uma entidade principal na mesma conta, nenhuma política baseada em identidade adicional será necessária. Consulte mais informações em Acesso a recursos entre contas no IAM no Guia do usuário do IAM.

Ações de política para mensagens sociais de usuário AWS final

Compatível com ações de políticas: sim

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

O elemento `Action` de uma política JSON descreve as ações que podem ser usadas para permitir ou negar acesso em uma política. As ações de política geralmente têm o mesmo nome da operação de AWS API associada. Existem algumas exceções, como ações somente de permissão, que não têm uma operação de API correspondente. Algumas operações também exigem várias ações em uma política. Essas ações adicionais são chamadas de ações dependentes.

Incluem ações em uma política para conceder permissões para executar a operação associada.

Para ver uma lista das ações sociais do AWS End User Messaging, consulte Ações definidas pelo AWS End User Messaging Social na Referência de Autorização do Serviço.

As ações de política no AWS End User Messaging Social usam o seguinte prefixo antes da ação:

```
social-messaging
```

Para especificar várias ações em uma única declaração, separe-as com vírgulas.

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

Para ver exemplos de políticas baseadas em identidade social para mensagens de usuário AWS final, consulte. Exemplos de políticas baseadas em identidade para redes sociais de mensagens de usuário AWS final

Recursos de política para mensagens sociais para usuários AWS finais

Compatível com recursos de políticas: sim

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

O elemento de política JSON `Resource` especifica o objeto ou os objetos aos quais a ação se aplica. As instruções devem incluir um elemento `Resource` ou `NotResource`. Como prática recomendada, especifique um recurso usando seu nome do recurso da Amazon (ARN). Isso pode ser feito para ações que oferecem compatibilidade com um tipo de recurso específico, conhecido como permissões em nível de recurso.

Para ações que não oferecem compatibilidade com permissões em nível de recurso, como operações de listagem, use um curinga (*) para indicar que a instrução se aplica a todos os recursos.

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

Para ver uma lista dos tipos de recursos sociais do AWS End User Messaging e seus ARNs, consulte Recursos definidos pelo AWS End User Messaging Social na Referência de Autorização do Serviço. Para saber com quais ações você pode especificar o ARN de cada recurso, consulte Ações definidas pelo AWS End User Messaging Social.

Para ver exemplos de políticas baseadas em identidade social para mensagens de usuário AWS final, consulte. Exemplos de políticas baseadas em identidade para redes sociais de mensagens de usuário AWS final

Chaves de condição de política para mensagens sociais de usuário AWS final

Compatível com chaves de condição de política específicas de serviço: sim

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

O elemento `Condition` (ou bloco `Condition`) permite que você especifique condições nas quais uma instrução estiver em vigor. O elemento `Condition` é opcional. É possível criar expressões condicionais que usem agentes de condição, como “igual a” ou “menor que”, para fazer a condição da política corresponder aos valores na solicitação.

Se você especificar vários elementos de `Condition` em uma declaração ou várias chaves em um único elemento de `Condition`, a AWS os avaliará usando uma operação lógica `AND`. Se você especificar vários valores para uma única chave de condição, AWS avalia a condição usando uma

0R operação lógica. Todas as condições devem ser atendidas antes que as permissões da instrução sejam concedidas.

Você também pode usar variáveis de espaço reservado ao especificar condições. Por exemplo, é possível conceder a um usuário do IAM permissão para acessar um recurso somente se ele estiver marcado com seu nome de usuário do IAM. Para obter mais informações, consulte Elementos da política do IAM: variáveis e tags no Guia do usuário do IAM.

AWS suporta chaves de condição globais e chaves de condição específicas do serviço. Para ver todas as chaves de condição AWS globais, consulte as chaves de contexto de condição AWS global no Guia do usuário do IAM.

Para ver uma lista das chaves de condição social do AWS End User Messaging, consulte Chaves de condição para AWS End User Messaging Social na Referência de Autorização do Serviço. Para saber com quais ações e recursos você pode usar uma chave de condição, consulte Ações definidas pelo usuário AWS final de mensagens sociais.

Para ver exemplos de políticas baseadas em identidade social para mensagens de usuário AWS final, consulte. Exemplos de políticas baseadas em identidade para redes sociais de mensagens de usuário AWS final

ACLs nas redes sociais de mensagens do usuário AWS final

Suportes ACLs: Não

As listas de controle de acesso (ACLs) controlam quais diretores (membros da conta, usuários ou funções) têm permissões para acessar um recurso. ACLs são semelhantes às políticas baseadas em recursos, embora não usem o formato de documento de política JSON.

ABAC com mensagens sociais para usuários AWS finais

Compatível com ABAC (tags em políticas): parcial

O controle de acesso por atributo (ABAC) é uma estratégia de autorização que define as permissões com base em atributos. Em AWS, esses atributos são chamados de tags. Você pode anexar tags a entidades do IAM (usuários ou funções) e a vários AWS recursos. Marcar de entidades e atributos é a primeira etapa do ABAC. Em seguida, você cria políticas de ABAC para permitir operações quando a tag da entidade principal corresponder à tag do recurso que ela estiver tentando acessar.

O ABAC é útil em ambientes que estão crescendo rapidamente e ajuda em situações em que o gerenciamento de políticas se torna um problema.

Para controlar o acesso baseado em tags, forneça informações sobre as tags no elemento de condição de uma política usando as `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` ou chaves de condição `aws:TagKeys`.

Se um serviço for compatível com as três chaves de condição para cada tipo de recurso, o valor será Sim para o serviço. Se um serviço for compatível com as três chaves de condição somente para alguns tipos de recursos, o valor será Parcial

Para obter mais informações sobre o ABAC, consulte Definir permissões com autorização do ABAC no Guia do usuário do IAM. Para visualizar um tutorial com etapas para configurar o ABAC, consulte Usar controle de acesso baseado em atributos (ABAC) no Guia do usuário do IAM.

Usando credenciais temporárias com o AWS End User Messaging Social

Compatível com credenciais temporárias: sim

Alguns Serviços da AWS não funcionam quando você faz login usando credenciais temporárias. Para obter informações adicionais, incluindo quais Serviços da AWS funcionam com credenciais temporárias, consulte Serviços da AWS “Trabalhe com o IAM” no Guia do usuário do IAM.

Você está usando credenciais temporárias se fizer login AWS Management Console usando qualquer método, exceto um nome de usuário e senha. Por exemplo, quando você acessa AWS usando o link de login único (SSO) da sua empresa, esse processo cria automaticamente credenciais temporárias. Você também cria automaticamente credenciais temporárias quando faz login no console como usuário e, em seguida, alterna perfis. Para obter mais informações sobre como alternar funções, consulte Alternar para um perfil do IAM (console) no Guia do usuário do IAM.

Você pode criar manualmente credenciais temporárias usando a AWS API AWS CLI ou. Em seguida, você pode usar essas credenciais temporárias para acessar AWS. AWS recomenda que você gere credenciais temporárias dinamicamente em vez de usar chaves de acesso de longo prazo. Para obter mais informações, consulte Credenciais de segurança temporárias no IAM.

Permissões principais entre serviços para mensagens sociais de usuário AWS final

Compatibilidade com o recurso de encaminhamento de sessões de acesso (FAS): sim

Quando você usa um usuário ou uma função do IAM para realizar ações AWS, você é considerado um principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. O FAS usa as permissões do diretor chamando um AWS service (Serviço da AWS), combinadas com a solicitação AWS service (Serviço da AWS) para fazer solicitações aos serviços posteriores. As solicitações do FAS são feitas somente quando um serviço recebe uma

solicitação que requer interações com outros Serviços da AWS ou com recursos para ser concluída. Nesse caso, você precisa ter permissões para executar ambas as ações. Para obter detalhes da política ao fazer solicitações de FAS, consulte Sessões de acesso direto.

Funções de serviço para mensagens sociais de usuário AWS final

Compatível com perfis de serviço: sim

O perfil de serviço é um perfil do IAM que um serviço assume para executar ações em seu nome. Um administrador do IAM pode criar, modificar e excluir um perfil de serviço do IAM. Para obter mais informações, consulte Criar um perfil para delegar permissões a um AWS service (Serviço da AWS) no Guia do Usuário do IAM.

> **Warning**
>
> Alterar as permissões de uma função de serviço pode interromper a funcionalidade social de mensagens do usuário AWS final. Edite as funções de serviço somente quando AWS o End User Messaging Social fornecer orientação para fazer isso.

Funções vinculadas a serviços para mensagens sociais de usuário AWS final

Compatibilidade com perfis vinculados a serviços: sim

Uma função vinculada ao serviço é um tipo de função de serviço vinculada a um. AWS service (Serviço da AWS) O serviço pode presumir o perfil de executar uma ação em seu nome. As funções vinculadas ao serviço aparecem em você Conta da AWS e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não editar as permissões para funções vinculadas ao serviço.

Para obter detalhes sobre como criar ou gerenciar perfis vinculados a serviços, consulte Serviços da AWS que funcionam com o IAM. Encontre um serviço na tabela que inclua um `Yes` na coluna Perfil vinculado ao serviço. Escolha o link Sim para visualizar a documentação do perfil vinculado a serviço desse serviço.

Exemplos de políticas baseadas em identidade para redes sociais de mensagens de usuário AWS final

Por padrão, usuários e funções não têm permissão para criar ou modificar recursos sociais de mensagens para usuários AWS finais. Eles também não podem realizar tarefas usando a AWS API

AWS Management Console, AWS Command Line Interface (AWS CLI) ou. Para conceder permissão aos usuários para executar ações nos recursos que eles precisam, um administrador do IAM pode criar políticas do IAM. O administrador pode então adicionar as políticas do IAM aos perfis e os usuários podem assumir os perfis.

Para aprender a criar uma política baseada em identidade do IAM ao usar esses documentos de política em JSON de exemplo, consulte Criar políticas do IAM (console) no Guia do usuário do IAM.

Para obter detalhes sobre ações e tipos de recursos definidos pelo AWS End User Messaging Social, incluindo o formato do ARNs para cada um dos tipos de recursos, consulte Ações, recursos e chaves de condição para AWS End User Messaging Social na Referência de Autorização de Serviço.

Tópicos

- Práticas recomendadas de política
- Usando o console social de mensagens para usuários AWS finais
- Permitir que os usuários visualizem suas próprias permissões

Práticas recomendadas de política

As políticas baseadas em identidade determinam se alguém pode criar, acessar ou excluir recursos sociais de mensagens de usuário AWS final em sua conta. Essas ações podem incorrer em custos para sua Conta da AWS. Ao criar ou editar políticas baseadas em identidade, siga estas diretrizes e recomendações:

- Comece com as políticas AWS gerenciadas e avance para as permissões de privilégios mínimos — Para começar a conceder permissões aos seus usuários e cargas de trabalho, use as políticas AWS gerenciadas que concedem permissões para muitos casos de uso comuns. Eles estão disponíveis no seu Conta da AWS. Recomendamos que você reduza ainda mais as permissões definindo políticas gerenciadas pelo AWS cliente que sejam específicas para seus casos de uso. Para obter mais informações, consulte Políticas gerenciadas pela AWS ou Políticas gerenciadas pela AWS para funções de trabalho no Guia do usuário do IAM.
- Aplique permissões de privilégio mínimo: ao definir permissões com as políticas do IAM, conceda apenas as permissões necessárias para executar uma tarefa. Você faz isso definindo as ações que podem ser executadas em recursos específicos sob condições específicas, também conhecidas como permissões de privilégio mínimo. Para obter mais informações sobre como usar o IAM para aplicar permissões, consulte Políticas e permissões no IAM no Guia do usuário do IAM.

- Use condições nas políticas do IAM para restringir ainda mais o acesso: você pode adicionar uma condição às políticas para limitar o acesso a ações e recursos. Por exemplo, você pode escrever uma condição de política para especificar que todas as solicitações devem ser enviadas usando SSL. Você também pode usar condições para conceder acesso às ações de serviço se elas forem usadas por meio de uma ação específica AWS service (Serviço da AWS), como AWS CloudFormation. Para obter mais informações, consulte Elementos da política JSON do IAM: condição no Guia do usuário do IAM.
- Use o IAM Access Analyzer para validar suas políticas do IAM a fim de garantir permissões seguras e funcionais: o IAM Access Analyzer valida as políticas novas e existentes para que elas sigam a linguagem de política do IAM (JSON) e as práticas recomendadas do IAM. O IAM Access Analyzer oferece mais de cem verificações de política e recomendações práticas para ajudar a criar políticas seguras e funcionais. Para obter mais informações, consulte Validação de políticas do IAM Access Analyzer no Guia do Usuário do IAM.
- Exigir autenticação multifator (MFA) — Se você tiver um cenário que exija usuários do IAM ou um usuário root, ative Conta da AWS a MFA para obter segurança adicional. Para exigir MFA quando as operações de API forem chamadas, adicione condições de MFA às suas políticas. Para obter mais informações, consulte Configuração de acesso à API protegido por MFA no Guia do Usuário do IAM.

Para obter mais informações sobre as práticas recomendadas do IAM, consulte Práticas recomendadas de segurança no IAM no Guia do usuário do IAM.

Usando o console social de mensagens para usuários AWS finais

Para acessar o console social do AWS End User Messaging, você deve ter um conjunto mínimo de permissões. Essas permissões devem permitir que você liste e visualize detalhes sobre os recursos sociais de mensagens do usuário AWS final em seu Conta da AWS. Caso crie uma política baseada em identidade mais restritiva que as permissões mínimas necessárias, o console não funcionará como pretendido para entidades (usuários ou perfis) com essa política.

Você não precisa permitir permissões mínimas do console para usuários que estão fazendo chamadas somente para a API AWS CLI ou para a AWS API. Em vez disso, permita o acesso somente a ações que correspondam à operação de API que estiverem tentando executar.

Para garantir que usuários e funções ainda possam usar o console social de mensagens de usuário AWS final, anexe também a política social de mensagens de usuário AWS final `ConsoleAccess`

ou a política *ReadOnly* AWS gerenciada às entidades. Para obter informações, consulte Adicionar permissões a um usuário no Guia do usuário do IAM.

Permitir que os usuários visualizem suas próprias permissões

Este exemplo mostra como criar uma política que permita que os usuários do IAM visualizem as políticas gerenciadas e em linha anexadas a sua identidade de usuário. Essa política inclui permissões para concluir essa ação no console ou programaticamente usando a API AWS CLI ou AWS .

```
{
    "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 políticas gerenciadas para redes sociais de mensagens de usuário AWS final

Para adicionar permissões a usuários, grupos e funções, é mais fácil usar políticas AWS gerenciadas do que escrever políticas você mesmo. É necessário tempo e experiência para criar políticas gerenciadas pelo cliente do IAM que fornecem à sua equipe apenas as permissões de que precisam. Para começar rapidamente, você pode usar nossas políticas AWS gerenciadas. Essas políticas abrangem casos de uso comuns e estão disponíveis na sua Conta da AWS. Para obter mais informações sobre políticas AWS gerenciadas, consulte políticas AWS gerenciadas no Guia do usuário do IAM.

AWS os serviços mantêm e atualizam as políticas AWS gerenciadas. Você não pode alterar as permissões nas políticas AWS gerenciadas. Os serviços ocasionalmente acrescentam permissões adicionais a uma política gerenciada pela AWS para oferecer suporte a novos recursos. Esse tipo de atualização afeta todas as identidades (usuários, grupos e funções) em que a política está anexada. É mais provável que os serviços atualizem uma política gerenciada pela AWS quando um novo recurso for iniciado ou novas operações se tornarem disponíveis. Os serviços não removem as permissões de uma política AWS gerenciada, portanto, as atualizações de políticas não violarão suas permissões existentes.

Além disso, AWS oferece suporte a políticas gerenciadas para funções de trabalho que abrangem vários serviços. Por exemplo, a política ReadOnlyAccess AWS gerenciada fornece acesso somente de leitura a todos os AWS serviços e recursos. Quando um serviço lança um novo recurso, AWS adiciona permissões somente de leitura para novas operações e recursos. Para obter uma lista e descrições das políticas de perfis de trabalho, consulte Políticas gerenciadas pela AWS para perfis de trabalho no Guia do usuário do IAM.

AWS Mensagens para o usuário final: atualizações sociais das políticas AWS gerenciadas

Veja detalhes sobre as atualizações das políticas AWS gerenciadas do AWS End User Messaging Social desde que esse serviço começou a rastrear essas alterações. Para receber alertas automáticos sobre alterações nessa página, assine o feed RSS na página de histórico do AWS End User Messaging Social Document.

Alteração	Descrição	Data
AWS O End User Messaging Social começou a monitorar as alterações	AWS O End User Messaging Social começou a monitorar as alterações em suas políticas AWS gerenciadas.	10 de outubro de 2024

Solução de problemas de mensagens de usuário AWS final: identidade social e acesso

Use as informações a seguir para ajudá-lo a diagnosticar e corrigir problemas comuns que você pode encontrar ao trabalhar com o AWS End User Messaging Social e o IAM.

Tópicos

- Não estou autorizado a realizar uma ação no AWS End User Messaging Social
- Não estou autorizado a realizar iam: PassRole
- Quero permitir que pessoas fora da minha acessem meus Conta da AWS recursos sociais de mensagens de usuário AWS final

Não estou autorizado a realizar uma ação no AWS End User Messaging Social

Se você receber uma mensagem de erro informando que não tem autorização para executar uma ação, suas políticas deverão ser atualizadas para permitir que você realize a ação.

O erro do exemplo a seguir ocorre quando o usuário do IAM `mateojackson` tenta usar o console para visualizar detalhes sobre um atributo *`my-example-widget`* fictício, mas não tem as permissões `social-messaging:`*`GetWidget`* fictícias.

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

Nesse caso, a política do usuário `mateojackson` deve ser atualizada para permitir o acesso ao recurso *`my-example-widget`* usando a ação `social-messaging:`*`GetWidget`*.

Se precisar de ajuda, entre em contato com seu AWS administrador. Seu administrador é a pessoa que forneceu suas credenciais de login.

Não estou autorizado a realizar iam: PassRole

Se você receber um erro informando que não está autorizado a realizar a `iam:PassRole` ação, suas políticas devem ser atualizadas para permitir que você passe uma função para o AWS End User Messaging Social.

Alguns Serviços da AWS permitem que você passe uma função existente para esse serviço em vez de criar uma nova função de serviço ou uma função vinculada ao serviço. Para fazer isso, é preciso ter permissões para passar o perfil para o serviço.

O exemplo de erro a seguir ocorre quando um usuário do IAM chamado `marymajor` tenta usar o console para realizar uma ação no AWS End User Messaging Social. No entanto, a ação exige que o serviço tenha permissões concedidas por um perfil de serviço. Mary não tem permissões para passar o perfil para o serviço.

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

Nesse caso, as políticas de Mary devem ser atualizadas para permitir que ela realize a ação `iam:PassRole`.

Se precisar de ajuda, entre em contato com seu AWS administrador. Seu administrador é a pessoa que forneceu suas credenciais de login.

Quero permitir que pessoas fora da minha acessem meus Conta da AWS recursos sociais de mensagens de usuário AWS final

É possível criar um perfil que os usuários de outras contas ou pessoas fora da sua organização podem usar para acessar seus recursos. É possível especificar quem é confiável para assumir o perfil. Para serviços que oferecem suporte a políticas baseadas em recursos ou listas de controle de acesso (ACLs), você pode usar essas políticas para conceder às pessoas acesso aos seus recursos.

Para saber mais, consulte:

- Para saber se o AWS End User Messaging Social oferece suporte a esses recursos, consulteComo o AWS End User Messaging Social funciona com o IAM.
- Para saber como fornecer acesso aos seus recursos em todos os Contas da AWS que você possui, consulte Como fornecer acesso a um usuário do IAM em outro Conta da AWS que você possui no Guia do usuário do IAM.
- Para saber como fornecer acesso aos seus recursos a terceiros Contas da AWS, consulte Como fornecer acesso Contas da AWS a terceiros no Guia do usuário do IAM.
- Para saber como conceder acesso por meio da federação de identidades, consulte Conceder acesso a usuários autenticados externamente (federação de identidades) no Guia do usuário do IAM.
- Para conhecer a diferença entre perfis e políticas baseadas em recurso para acesso entre contas, consulte Acesso a recursos entre contas no IAM no Guia do usuário do IAM.

Validação de conformidade para mensagens sociais de usuário AWS final

Para saber se um AWS service (Serviço da AWS) está dentro do escopo de programas de conformidade específicos, consulte Serviços da AWS Escopo por Programa de Conformidade Serviços da AWS e escolha o programa de conformidade em que você está interessado. Para obter informações gerais, consulte Programas de AWS conformidade Programas AWS de .

Você pode baixar relatórios de auditoria de terceiros usando AWS Artifact. Para obter mais informações, consulte Baixar relatórios em AWS Artifact .

Sua responsabilidade de conformidade ao usar Serviços da AWS é determinada pela confidencialidade de seus dados, pelos objetivos de conformidade de sua empresa e pelas leis e regulamentações aplicáveis. AWS fornece os seguintes recursos para ajudar na conformidade:

- Governança e conformidade de segurança: esses guias de implementação de solução abordam considerações sobre a arquitetura e fornecem etapas para implantar recursos de segurança e conformidade.
- Referência de serviços qualificados para HIPAA: lista os serviços qualificados para HIPAA. Nem todos Serviços da AWS são elegíveis para a HIPAA.
- AWS Recursos de https://aws.amazon.com/compliance/resources/ de conformidade — Essa coleção de pastas de trabalho e guias pode ser aplicada ao seu setor e local.

- AWS Guias de conformidade do cliente — Entenda o modelo de responsabilidade compartilhada sob a ótica da conformidade. Os guias resumem as melhores práticas de proteção Serviços da AWS e mapeiam as diretrizes para controles de segurança em várias estruturas (incluindo o Instituto Nacional de Padrões e Tecnologia (NIST), o Conselho de Padrões de Segurança do Setor de Cartões de Pagamento (PCI) e a Organização Internacional de Padronização (ISO)).
- Avaliação de recursos com regras no Guia do AWS Config desenvolvedor — O AWS Config serviço avalia o quão bem suas configurações de recursos estão em conformidade com as práticas internas, as diretrizes e os regulamentos do setor.
- AWS Security Hub— Isso AWS service (Serviço da AWS) fornece uma visão abrangente do seu estado de segurança interno AWS. O Security Hub usa controles de segurança para avaliar os recursos da AWS e verificar a conformidade com os padrões e as práticas recomendadas do setor de segurança. Para obter uma lista dos serviços e controles aceitos, consulte a Referência de controles do Security Hub.
- Amazon GuardDuty — Isso AWS service (Serviço da AWS) detecta possíveis ameaças às suas cargas de trabalho Contas da AWS, contêineres e dados monitorando seu ambiente em busca de atividades suspeitas e maliciosas. GuardDuty pode ajudá-lo a atender a vários requisitos de conformidade, como o PCI DSS, atendendo aos requisitos de detecção de intrusões exigidos por determinadas estruturas de conformidade.
- AWS Audit Manager— Isso AWS service (Serviço da AWS) ajuda você a auditar continuamente seu AWS uso para simplificar a forma como você gerencia o risco e a conformidade com as regulamentações e os padrões do setor.

Resiliência nas mensagens AWS sociais do usuário final

A infraestrutura AWS global é construída em torno Regiões da AWS de zonas de disponibilidade. Regiões da AWS fornecem várias zonas de disponibilidade fisicamente separadas e isoladas, conectadas a redes de baixa latência, alta taxa de transferência e alta redundância. Com as zonas de disponibilidade, é possível projetar e operar aplicações e bancos de dados que automaticamente executam o failover entre as zonas sem interrupção. As zonas de disponibilidade são altamente disponíveis, tolerantes a falhas e escaláveis que uma ou várias infraestruturas de data center tradicionais.

Para obter mais informações sobre zonas de disponibilidade Regiões da AWS e zonas de disponibilidade, consulte Infraestrutura AWS global.

Além da infraestrutura AWS global, o AWS End User Messaging Social oferece vários recursos para ajudar a suportar suas necessidades de resiliência e backup de dados.

Segurança da infraestrutura nas redes sociais de mensagens do usuário AWS final

Como um serviço gerenciado, o AWS End User Messaging Social é protegido pelos procedimentos AWS globais de segurança de rede descritos no whitepaper Amazon Web Services: Overview of Security Processes.

Você usa chamadas de API AWS publicadas para acessar o AWS End User Messaging Social por meio da rede. Os clientes devem oferecer compatibilidade com Transport Layer Security (TLS) 1.0 ou posterior. Recomendamos usar o TLS 1.2 ou posterior. Os clientes também devem ter suporte a conjuntos de criptografia com perfect forward secrecy (PFS) como DHE (Ephemeral Diffie-Hellman) ou ECDHE (Ephemeral Elliptic Curve Diffie-Hellman). A maioria dos sistemas modernos, como Java 7 e versões posteriores, comporta esses modos.

Além disso, as solicitações devem ser assinadas usando um ID da chave de acesso e uma chave de acesso secreta associada a uma entidade principal do IAM. Ou é possível usar o AWS Security Token Service (AWS STS) para gerar credenciais de segurança temporárias para assinar solicitações.

Prevenção contra o ataque do “substituto confuso” em todos os serviços

“Confused deputy” é um problema de segurança no qual uma entidade sem permissão para executar uma ação pode coagir uma entidade mais privilegiada a executá-la. Em AWS, a falsificação de identidade entre serviços pode resultar no problema confuso do deputado. A personificação entre serviços pode ocorrer quando um serviço (o serviço de chamada) chama outro serviço (o serviço chamado). O serviço de chamada pode ser manipulado de modo a usar suas permissões para atuar nos recursos de outro cliente de uma forma na qual ele não deveria ter permissão para acessar. Para evitar isso, a AWS fornece ferramentas que ajudam você a proteger seus dados para todos os serviços com entidades principais de serviço que receberam acesso aos recursos em sua conta.

Recomendamos usar as chaves de contexto de condição `aws:SourceAccount`global `aws:SourceArn`e as chaves de contexto nas políticas de recursos para limitar as permissões que

o Social Messaging concede a outro serviço ao recurso. Use `aws:SourceArn` se quiser apenas um recurso associado a acessibilidade de serviço. Use `aws:SourceAccount` se quiser permitir que qualquer recurso nessa conta seja associado ao uso entre serviços.

A maneira mais eficaz de se proteger contra o problema do substituto confuso é usar a chave de contexto de condição global `aws:SourceArn` com o ARN completo do recurso. Se você não souber o ARN completo do recurso ou especificar vários recursos, use a chave de condição de contexto global `aws:SourceArn` com caracteres curinga (*) para as partes desconhecidas do ARN. Por exemplo, `arn:aws:social-messaging:*:123456789012:*`.

Se o valor de `aws:SourceArn` não contiver o ID da conta, como um ARN de bucket do Amazon S3, você deverá usar ambas as chaves de contexto de condição global para limitar as permissões.

O valor de `aws:SourceArn` deve ser ResourceDescription.

O exemplo a seguir mostra como você pode usar as chaves de contexto de condição `aws:SourceAccount` global `aws:SourceArn` e as chaves de contexto no Social Messaging para evitar o confuso problema do substituto.

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

Práticas recomendadas de segurança

AWS O End User Messaging Social fornece vários recursos de segurança a serem considerados ao desenvolver e implementar suas próprias políticas de segurança. As práticas recomendadas a seguir são diretrizes gerais e não representam uma solução completa de segurança. Como essas práticas recomendadas podem não ser adequadas ou suficientes para o seu ambiente, trate-as como considerações úteis em vez de prescrições.

- Crie um usuário individual para cada pessoa que gerencia os recursos sociais do AWS End User Messaging, incluindo você mesmo. Não use credenciais AWS raiz para gerenciar recursos sociais de mensagens de usuário AWS final.
- Conceda a cada usuário o conjunto mínimo de permissões necessárias para realizar suas funções.
- Use grupos do IAM para gerenciar efetivamente permissões para vários usuários.
- Mude suas credenciais do IAM regularmente.

Usando funções vinculadas a serviços para mensagens sociais de usuário AWS final

AWS O End User Messaging Social usa AWS Identity and Access Management funções vinculadas ao serviço (IAM). Uma função vinculada ao serviço é um tipo exclusivo de função do IAM vinculada diretamente ao AWS End User Messaging Social. As funções vinculadas ao serviço são predefinidas pelo AWS End User Messaging Social e incluem todas as permissões que o serviço exige para chamar outros AWS serviços em seu nome.

Uma função vinculada ao serviço facilita a configuração do AWS End User Messaging Social porque você não precisa adicionar manualmente as permissões necessárias. AWS O End User Messaging Social define as permissões de suas funções vinculadas ao serviço e, a menos que seja definido de outra forma, somente o AWS End User Messaging Social pode assumir suas funções. As permissões definidas incluem a política de confiança e a política de permissões, e essa política não pode ser anexada a nenhuma outra entidade do IAM.

Uma função vinculada ao serviço poderá ser excluída somente após excluir seus recursos relacionados. Isso protege seus recursos sociais de mensagens de usuário AWS final porque você não pode remover inadvertidamente a permissão para acessar os recursos.

Para obter informações sobre outros serviços que oferecem suporte a funções vinculadas a serviços, consulte AWS Serviços que funcionam com IAM e procure os serviços que têm Sim na coluna

Funções vinculadas ao serviço. Escolha um Sim com um link para visualizar a documentação da função vinculada a esse serviço.

Permissões de função vinculadas ao serviço para mensagens sociais de usuário AWS final

AWS O End User Messaging Social usa a função vinculada ao serviço chamada AWSServiceRoleForSocialMessaging— Para publicar métricas e fornecer informações sobre o envio de suas mensagens sociais.

A função AWSService RoleForSocialMessaging vinculada ao serviço confia nos seguintes serviços para assumir a função:

- `social-messaging.amazonaws.com`

A política de permissões de função denominada AWSSocial MessagingServiceRolePolicy permite que o AWS End User Messaging Social conclua as seguintes ações nos recursos especificados:

- Ação: `"cloudwatch:PutMetricData"` em `all AWS resources in the AWS/SocialMessaging namespace.`

Você deve configurar permissões para permitir que seus usuários, grupos ou perfis criem, editem ou excluam um perfil vinculado ao serviço. Para obter mais informações, consulte Service-linked role permissions (Permissões de nível vinculado a serviços) no Guia do usuário do IAM.

Para atualizações da política, consulteAWS Mensagens para o usuário final: atualizações sociais das políticas AWS gerenciadas.

Criação de uma função vinculada ao serviço para o AWS End User Messaging Social

Você pode usar o console do IAM para criar uma função vinculada ao serviço com o caso de uso AWSEndUserMessagingSocial - Metrics. Na AWS CLI ou na AWS API, crie uma função vinculada ao serviço com o nome do `social-messaging.amazonaws.com` serviço. Para obter mais informações, consulte Criar uma função vinculada ao serviço no Manual do usuário do IAM. Se você excluir essa função vinculada ao serviço, será possível usar esse mesmo processo para criar a função novamente.

Você pode criar a função vinculada ao serviço para AWS End User Messaging Social com o seguinte comando: AWS CLI

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

Editando uma função vinculada ao serviço para AWS End User Messaging Social

AWS O End User Messaging Social não permite que você edite a função AWSService RoleForSocialMessaging vinculada ao serviço. Depois que criar um perfil vinculado ao serviço, você não poderá alterar o nome do perfil, pois várias entidades podem fazer referência a ele. No entanto, será possível editar a descrição do perfil usando o IAM. Para obter mais informações, consulte Editar um perfil vinculado ao serviço no Guia do usuário do IAM.

Excluindo uma função vinculada ao serviço para AWS End User Messaging Social

Se você não precisar mais usar um atributo ou serviço que requer uma função vinculada a serviço, é recomendável excluí-la. Dessa forma, você não tem uma entidade não utilizada que não seja monitorada ativamente ou mantida. No entanto, você deve limpar os recursos de seu perfil vinculado ao serviço antes de excluí-lo manualmente.

> **Note**
>
> Se o serviço social de mensagens de usuário AWS final estiver usando a função quando você tentar excluir os recursos, a exclusão poderá falhar. Se isso acontecer, espere alguns minutos e tente a operação novamente.

Para remover os recursos sociais de mensagens do usuário AWS final usados pelo AWSService RoleForSocialMessaging

1. Chame a `list-linked-whatsapp-business-accounts` API para ver os recursos que você tem.
2. Para cada conta comercial vinculada do Whats App, chame a `disassociate-whatsapp-business-account` API para remover o recurso do SocialMessaging serviço.

3. Verifique se nenhum recurso foi retornado chamando a `list-linked-whatsapp-business-accounts` API novamente.

Como excluir manualmente o perfil vinculado ao serviço usando o IAM

Use o console do IAM AWS CLI, o ou a AWS API para excluir a função AWSService RoleForSocialMessaging vinculada ao serviço. Para obter mais informações, consulte Excluir um perfil vinculado ao serviço no Guia do usuário do IAM.

Regiões suportadas para funções AWS vinculadas ao serviço social de mensagens de usuário final

AWS O End User Messaging Social oferece suporte ao uso de funções vinculadas ao serviço em todas as regiões em que o serviço está disponível. Para obter mais informações, consulte Regiões e endpoints da AWS.

Acesse AWS o End User Messaging Social usando um endpoint de interface ()AWS PrivateLink

Você pode usar AWS PrivateLink para criar uma conexão privada entre você VPC e o AWS End User Messaging Social. Você pode acessar o AWS End User Messaging Social como se estivesse no seuVPC, sem o uso de um gateway de internet, NAT dispositivo, VPN conexão ou AWS Direct Connect conexão. Suas instâncias VPC não precisam de endereços IP públicos para acessar o AWS End User Messaging Social.

Você estabelece essa conectividade privada criando um endpoint de interface, desenvolvido pelo AWS PrivateLink. Criaremos um endpoint de interface de rede em cada sub-rede que você habilitar para o endpoint de interface. Essas são interfaces de rede gerenciadas pelo solicitante que servem como ponto de entrada para o tráfego destinado ao AWS End User Messaging Social.

Para obter mais informações, consulte Acesso Serviços da AWS por meio AWS PrivateLink do AWS PrivateLink Guia.

Considerações sobre mensagens AWS sociais para usuários finais

Antes de configurar um endpoint de interface para o AWS End User Messaging Social, analise as Considerações no AWS PrivateLink Guia.

AWS O End User Messaging Social suporta a realização de chamadas para todas as suas API ações por meio do endpoint da interface.

VPCas políticas de endpoint não são suportadas pelo AWS End User Messaging Social. Por padrão, o acesso total ao AWS End User Messaging Social é permitido por meio do endpoint da interface. Como alternativa, você pode associar um grupo de segurança às interfaces de rede do endpoint para controlar o tráfego para o AWS End User Messaging Social por meio do endpoint da interface.

Crie um endpoint de interface para mensagens sociais de usuário AWS final

Você pode criar um endpoint de interface para o AWS End User Messaging Social usando o VPC console da Amazon ou o AWS Command Line Interface (AWS CLI). Para obter mais informações, consulte Criar um endpoint de interface no Guia do usuário do AWS PrivateLink .

Crie um endpoint de interface para AWS End User Messaging Social usando o seguinte nome de serviço:

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

Se você habilitar privado DNS para o endpoint da interface, poderá fazer API solicitações ao AWS End User Messaging Social usando seu DNS nome regional padrão. Por exemplo, `service-name.us-east-1.amazonaws.com`.

Crie uma política de endpoint para seu endpoint de interface.

Uma política de endpoint é um IAM recurso que você pode anexar a um endpoint de interface. A política de endpoint padrão permite acesso total ao AWS End User Messaging Social por meio do endpoint da interface. Para controlar o acesso permitido ao AWS End User Messaging Social a partir do seuVPC, anexe uma política de endpoint personalizada ao endpoint da interface.

Uma política de endpoint especifica as seguintes informações:

- Os diretores que podem realizar ações (Contas da AWS, IAM usuários e IAM funções).
- As ações que podem ser realizadas.
- Os recursos nos quais as ações podem ser executadas.

Para obter mais informações, consulte Controlar o Acesso a Serviços Usando Políticas de Endpoint no AWS PrivateLink Guia.

Exemplo: política de VPC endpoint para ações sociais de mensagens de usuário AWS final

O exemplo a seguir refere-se a uma política de endpoint personalizada. Quando você anexa essa política ao seu endpoint de interface, ela concede acesso às ações sociais de mensagens do usuário AWS final listadas para todos os diretores em todos os recursos.

```
{
   "Statement": [
      {
         "Principal": "*",
         "Effect": "Allow",
         "Action": [
            "social-messaging:DeleteWhatsAppMessageMedia",
```

```
            "social-messaging:PostWhatsAppMessageMedia",
            "social-messaging:SendWhatsAppMessage"
         ],
         "Resource":"*"
      }
   ]
}
```

Cotas para mensagens sociais para usuários AWS finais

Sua AWS conta tem cotas padrão, anteriormente chamadas de limites, para cada AWS serviço. A menos que especificado de outra forma, cada cota é específica da região . É possível solicitar aumentos para algumas cotas e outras cotas não podem ser aumentadas.

Sua AWS conta tem as seguintes cotas relacionadas ao AWS End User Messaging Social.

Recurso	Padrão
WhatsApp Conta comercial (WABA)	25 por região

AWS O End User Messaging Social implementa cotas que restringem o número de solicitações que você pode fazer ao AWS End User Messaging Social a API partir do seu. Conta da AWS

Operation	Cota de taxa padrão (solicitações por segundo)
SendWhatsAppMessage	1.000
PostWhatsAppMessageMedia	100
GetWhatsAppMessageMedia	100
DeleteWhatsAppMessageMedia	100
DisassociateWhatsAppBusinessAccount	10
ListWhatsAppBusinessAccount	10
TagResource	10
UntagResourceRate	10
ListTagsForResourceRate	10

Histórico de documentos do Guia do usuário do AWS End User Messaging Social

A tabela a seguir descreve as versões da documentação do AWS End User Messaging Social.

Alteração	Descrição	Data
Disponibilidade regional	Foi adicionado suporte para a região da Europa (Frankfurt). Para obter mais informações, consulte Disponibilidade regional.	5 de dezembro de 2024
Adicione uma mensagem e um destino para o evento	Foi adicionado suporte para o Amazon Connect como destino de eventos. Para obter mais informações, consulte Adicionar uma mensagem e um destino para o evento.	1.º de dezembro de 2024
AWS PrivateLink	Foi adicionado suporte para AWS PrivateLink. Para obter mais informações, consulte AWS PrivateLink.	22 de outubro de 2024
Lançamento inicial	Versão inicial do Guia do usuário do AWS End User Messaging Social	10 de outubro de 2024

As traduções são geradas por tradução automática. Em caso de conflito entre o conteúdo da tradução e da versão original em inglês, a versão em inglês prevalecerá.