Manual do usuário

AWS Mensagens sociais para o usuário final

AWS Mensagens sociais para o usuário final: Manual do usuário

Table of Contents

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 avançados 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 de WhatsApp mensagens aos seus aplicativos junto com os canais existentes, como SMS notificações push, permitindo que você interaja com os clientes por meio do canal de comunicação preferido deles.

Para começar, você pode criar uma nova conta WhatsApp comercial (WABA) usando o processo de integração autoguiado no console social do AWS End User Messaging ou vincular uma existente WABA ao serviço.

Tópicos

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

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

- 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 recursos e as funcionalidades a seguir:

- 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 em mensagens enviadas.
- Acesso a novos 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 de usuário AWS final SMS para enviar SMS mensagens
- Use o envio de mensagens push para o usuário AWS final para enviar notificações push
- Use SES a Amazon para enviar e-mails

Acessando mensagens sociais para usuários AWS finais

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 AWS serviços da usando comandos no shell da linha de comando. A 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 AWS SMS comandos na Referência de AWS CLI Comandos.

AWS SDKs

Se você for um desenvolvedor de software que prefere criar aplicativos usando uma linguagem APIs em vez de enviar uma solicitação via HTTP ouHTTPS, a AWS fornece bibliotecas, código de exemplo, tutoriais e outros recursos. Essas bibliotecas fornecem funções básicas que automatizam tarefas, como assinatura criptografada de suas solicitações, novas tentativas de solicitações e tratamento das respostas de erro. Essas funções ajudam você a começar. Para obter mais informações, consulte Ferramentas para criar na AWS.

Disponibilidade regional

AWS O End User Messaging Social está disponível Regiões da AWS em várias redes sociais da na América do Norte, Europa, Ásia e Oceania. Em cada região, a 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 níveis muito altos 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 disponível atualmente e o endpoint de cada região, consulte Endpoints e cotas para Endpoints de serviço e Endpoints de AWS serviço para o AWS End User Messaging Social API na tabela Referência geral da Amazon Web Servicesou na tabela a seguir. 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 APIversão
Leste dos EUA (Norte da Virgínia)	us-east-1	social-messaging.us-east-1.amazonaws.com social-messaging-fips.api.aws social-api.aws	Versão 20 e posterior

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

Nome da região	Região	Endpoint	WhatsApp APIversão
Europa (Londres)	eu-west-2	social-messaging.eu-west-2.amazonaws.com social-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, siga as etapas abaixo.

Tópicos

Cadastrar-se em uma Conta da AWS

Se você ainda não tem uma Conta da AWS, siga as etapas a seguir para criar uma.

Para cadastrar-se em uma 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 atributos 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 A envia um e-mail de confirmação depois que o processo de cadastramento é concluído. A qualquer momento, é possível visualizar as atividades da conta atual e gerenciar sua conta acessando https://aws.amazon.com/e selecionando My Account (Minha conta).

Criar um usuário com acesso administrativo

Depois de cadastrar uma Conta da AWS, proteja seu Usuário raiz da conta da AWS, proteja seu AWS IAM Identity Center, habilite o e crie um usuário administrativo para não usar o usuário raiz em tarefas cotidianas.

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 sua 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. Habilitar a autenticação multifator (MFA) para o usuário raiz.

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

Criar um usuário com acesso administrativo

1. Habilitar o IAM Identity Center.

   Para obter instruções, consulte Habilitar AWS IAM Identity Center no Guia do usuário do AWS IAM Identity Center .
2. No Centro de IAM Identidade, conceda o acesso administrativo para 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 seu usuário do Centro de IAM Identidade, use o login URL que foi enviado ao seu endereço de email quando você criou o usuário do Centro do IAM Usuário.

  Para obter ajuda com o login utilizando um usuário do Centro de IAM Identidade, consulte Início de sessão no portal de AWS acesso da, no Guia do Início de Sessão da AWS usuário do.

Atribuir acesso a usuários adicionais

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

Para obter instruções, consulte Create a permission set 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 Add groups 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

Cadastro na 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. A WABA contém seus 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 nesta seção para começar a usar o AWS End User Messaging Social. Use o processo de inscrição incorporado para criar uma nova conta WhatsApp comercial (WABA) ou migrar uma existente WABA 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 WhatsApp e.

- Você deve criar uma conta de gerente de negócios com o Meta e vinculá-la à suaWABA.
- Você deve fornecer o controle do seu WABA para nós. A seu pedido, transferiremos o controle de suas WABA costas 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 e/ou limitações na distribuição de acordo com as leis e/ou regulamentos aplicáveis.
- 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 tem uma conta Meta Business, você pode criar uma durante o processo de cadastro.
- 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 uma senha de uso único SMS ou de voz ()OTP. 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 paraSMS,MMS, e mensagens de voz.
- Se você estiver importando um existenteWABA, precisará do PINs para todos os números de telefone associados ao importadoWABA. Para redefinir um item perdido ou esquecidoPIN, siga as instruções em Atualização PIN na WhatsApp Business Platform Cloud API Reference.

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 existenteWABA. 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 comercial (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 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 site da sua empresa ou, se sua empresa não tiver um site, insira o na URL 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 a 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 usar 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 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.

Tags são pares de chaves e valores que você pode aplicar opcionalmente aos seus AWS recursos da para controlar o acesso ou o uso. Escolha Adicionar nova tag e insira um par chave-valor 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 ativar o registro de eventos na AmazonSNS, 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 a AmazonSNS, escolha Novo tópico SNS padrão da Amazon e insira um nome em Nome do tópico, ou escolha Tópico SNS padrão existente da Amazon e escolha um tópico na lista suspensa Tópico arn.

17. Em Números de telefone:

    Para cada número de telefone em Números de WhtsApp telefone:

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

    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 API local em nuvem na WhatsApp Business Platform Cloud API Reference.

ii. Tags são pares de chaves e valores que você pode aplicar opcionalmente aos seus AWS recursos da para controlar o acesso ou o uso. Escolha Adicionar nova tag e insira um par chave-valor 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 na AmazonSNS, 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. Para a AmazonSNS, escolha Novo tópico SNS padrão da Amazon e insira um nome em Nome do tópico, ou escolha Tópico SNS padrão existente da Amazon e escolha um tópico na lista suspensa Tópico arn.

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

Próximas etapas

Depois de concluir a cadastro, você poderá 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

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 Meta. Uma conta WhatsApp comercial contém ativos voltados para o cliente, como número de telefone, modelos e informações de contato comercial. A só WABA pode existir em um Região da AWS. Para obter mais informações sobre contas WhatsApp comerciais, consulte Contas WhatsApp comerciais na WhatsApp Business Platform Cloud API Reference.

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 WhatsApp e.
- Você deve criar uma conta de gerente de negócios com o Meta e vinculá-la à suaWABA.
- Você deve fornecer o controle do seu WABA para nós. A seu pedido, transferiremos o controle de suas WABA costas 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 e/ou limitações na distribuição de acordo com as leis e/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) no AWS End User Messaging Social

Siga estas instruções para ver o WABA associado a você Conta da AWS.

1. Abra o console social do AWS End User Messaging em https://console.aws.amazon.com/social-messaging/.
2. Em Contas comerciais, escolha umaWABA.
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 no 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 um WABA tem um limite de 250 modelos.

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

Adicionar uma conta WhatsApp comercial (WABA) no AWS End User Messaging Social

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 aoWABA.

- Para adicionar um novo WABA à sua conta, siga as etapas emIntrodução ao AWS End User Messaging Social:
  - Na etapa 8, escolha seu perfil WhatsApp comercial e 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 de Negócios:

- 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 os usuários, mesmo que eles não tenham adicionado a empresa ao catálogo de endereços. Esse recurso ajuda os usuários a identificar contas comerciais verificadas em WhatsApp.
- Conta comercial oficial: junto com os 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 conhecida e reconhecida pelos consumidores, por meio de artigos, postagens em blogs ou avaliações independentes. A aprovação de um não WhatsApp OBA 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 uma WhatsApp 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 só é exibido 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 WhatsApp Business Platform Cloud API Reference.
- Para obter mais informações sobre o processo de verificação comercial, consulte Verificação comercial na WhatsApp Business Platform Cloud API Reference.

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

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

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

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

1. Verifique se o país ou a região do número de telefone oferece suporte bidirecionalSMS.
2. Solicite o número de telefone. Dependendo do país ou da região, talvez seja necessário registrar o número de telefone.

3. Ative o envio de SMS mensagens bidirecionais para o número de telefone. Quando a configuração estiver concluída, suas SMS mensagens 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, certifique-se de que os seguintes pré-requisitos sejam atendidos:

- O número de telefone deve ser capaz de receber uma senha de uso único SMS ou de voz ()OTP. Este é o número de telefone que é adicionado ao seuWABA.
- O número de telefone não deve estar associado a nenhum outroWABA.

Adicione um número de telefone a um WABA

Para adicionar um novo número de telefone ao seu número existente WABA

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 perfil WhatsApp comercial ao qual 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 WhtsApp telefone:

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

    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 API local em nuvem na WhatsAppBusiness Platform Cloud API Reference.

        ii. Tags: pares de chaves e valores que você pode aplicar opcionalmente aos seus AWS recursos da para controlar o acesso ou o uso. Escolha Adicionar nova tag e insira um par chave-valor da 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 na AmazonSNS, 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. Para a AmazonSNS, escolha Novo tópico SNS padrão da Amazon e insira um nome em Nome do tópico, ou escolha Tópico SNS padrão existente da Amazon e escolha um tópico na lista suspensa Tópico arn.

13. 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 7 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 de número de telefone

- Conectado: você pode enviar mensagens dentro do seu limite de mensagens.
- Sinalizado: a qualidade do seu número de telefone está baixa e precisa ser melhorada. Se a qualidade do seu telefone não melhorar em 7 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, mas ainda pode responder às mensagens recebidas dos clientes. Quando o período de 24 horas terminar, você poderá enviar mensagens novamente.

Exibir uma classificação de qualidade de 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 umaWABA.
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 no dia.

Usando modelos de mensagem no AWS End User Messaging Social

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 em local
- 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 do AWS End User Messaging em https://console.aws.amazon.com/social-messaging/.

2. Escolha Conta comercial e, em seguida, escolha umaWABA.
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 análise 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 feedback negativo do cliente. 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 Modelo de ritmo na WhatsApp Business Platform Cloud API Reference.

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 do AWS End User Messaging em https://console.aws.amazon.com/social-messaging/.
2. Escolha Conta comercial e, em seguida, escolha umaWABA.
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 WhatsApp Business Platform Cloud API Reference.

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.

Status do modelo	Classificação de qualidade	Significado
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	Alta	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.

Status do modelo	Classificação de qualidade	Significado
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, 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.
Apelação solicitada		Foi solicitado o recurso.

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 WhatsApp Business Platform Cloud API Reference.

Destinos de mensagens e eventos no AWS End User Messaging Social

O destino de um evento é um SNS tópico da Amazon para o qual os WhatsApp eventos são enviados. Quando você ativa a publicação de eventos em um SNS tópico da Amazon, todos os seus eventos de envio e recebimento são enviados para o SNS tópico da Amazon. 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

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

Pré-requisitos

Antes de começar, certifique-se de que os seguintes pré-requisitos sejam atendidos.

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

Adicionar uma mensagem e o destino do 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 umaWABA.
3. Na guia Destino do evento, escolha Editar destino.
4. Para ativar o destino de um evento, escolha Habilitar.
5. Para enviar seus eventos para um novo SNS destino da Amazon, escolha Novo tópico do SNS estande e insira um nome em Nome do tópico. O SNS tópico da Amazon foi criado com permissões para permitir que o AWS End User Messaging Social acesse o tópico.

   Para enviar seus eventos para um SNS destino existente na Amazon, escolha Tópico SNS padrão existente e escolha um tópico em Tópico arn. Você precisa aplicar as seguintes permissões ao SNS tópico da Amazon:

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

Políticas de SNS tópicos criptografadas da Amazon

Você pode usar SNS tópicos da Amazon 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 SNS tópicos da Amazon usando AWS KMS chaves, consulte Ativar a compatibilidade entre as fontes de eventos de AWS serviços da e tópicos criptografados no Guia do desenvolvedor do Amazon Simple Notification Service.

O exemplo de declaração usa as `SourceArn` condições, que são opcionais, mas `SourceAccount` recomendadas, para evitar o confuso problema do substituto. 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 IAM do usuário.

A chave que você usa deve ser simétrica. SNSTópicos criptografados da Amazon não oferecem suporte a chaves assimétricas AWS KMS .

A política de chave 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}:*"
        }
     }
}
```

Próximas etapas

Depois de configurado, assine um endpoint para o tópico. SNS O endpoint começará a receber mensagens publicadas no tópico associado. Para obter mais informações sobre como se inscrever em um tópico, consulte Assinatura de um SNS tópico da Amazon no Amazon SNS Developer Guide.

Formato de mensagem e evento no AWS End User Messaging Social

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

AWS Cabeçalho do evento social de mensagens para o usuário final

O JSON objeto de um evento contém o cabeçalho do AWS evento WhatsApp JSON e. 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 WABA id do 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 WhatsApp JSON de recebimento de 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 obter uma lista dos campos e seus significados, consulte Referência de carga útil de notificação de webhooks na WhatsApp Business Platform Cloud Reference. API

```
{
//AWS End User Messaging Social header
}
{
  "id": "365731266123456",
  "changes": [
    {
      "value": {
        "messaging_product": "whatsapp",
        "metadata": {
          "display_phone_number": "12065550100",
          "phone_number_id": "321010217760100"
        },
        "contacts": [
          {
            "profile": {
              "name": "Diego"
            },
            "wa_id": "12065550102"
          }
        ],
        "messages": [
          {
            "from": "14255550150",
            "id":
 "wamid.HBgLMTQyNTY5ODgzMDIVAgASGCBDNzBDRjM5MDU2ODEwMDkwREY4ODBDRDE0RjVGRkexample",
            "timestamp": "1723506035",
            "text": {
              "body": "Hi"
            },
            "type": "text"
          }
        ]
      },
```

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

Exemplo WhatsApp JSON de recebimento de 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 GetWhatsAppMessageMedia API comando. 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. 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 URL compilá-lo no arquivo. Para obter mais informações sobre os comandos do Amazon S3, consulte Uso de comandos de alto nível (s3) com o. AWS CLI Para obter mais informações sobre como configurar o AWS CLI, consulte Configurar o 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.

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

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:

- Substituir *us-east-1* com Região da AWS aquele em que você WABA está.
- Substituir *BucketName* pelo nome do novo bucket.

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:

- Substituir *SourceFilePathAndName* pelo caminho e pelo nome do arquivo para o caminho e o nome do arquivo a ser copiado.
- Substituir *BucketName* pelo nome do bucket.
- Substituir *FileName* com o nome a ser usado para o arquivo.

O URL a ser usado ao enviar é:

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

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

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

Tipos e tamanhos de arquivos de mídia suportados em WhatsApp

Ao enviar ou receber uma mensagem de mídia, o tipo de arquivo deve ser suportado 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 arquivos de mídia

Formatos de áudio

Tipo de áudio	Extensão	MIMETipo	Tamanho máx.
AAC	.aac	audio/aac	16 MB
AMR	.amr	audio/amr	16 MB
MP3	.mp3	audio/mpeg	16 MB
MP4Áudio	.m4a	audio/mp4	16 MB
OGGÁudio	.ogg	audio/ogg	16 MB

Formatos de documentos

Tipo de documento	Extensão	MIMETipo	Tamanho máx.
Texto	.text	text/plain	100 MB
Microsoft Excel	.xls, .xlsx	aplicativo/vnd.ms-excel, aplicativo/vnd.openxmlformats-officedocument.spreadsheetml.sheet	100 MB
Microsoft Word	.doc, .docx	aplicativo/msword, aplicativo/vnd.openxmlformats-officedocument.wordprocessingml.document	100 MB
Microsoft PowerPoint	.ppt, .pptx	aplicativo/vnd.ms-powerpoint, aplicativo/vnd.openxmlformats-officedocument.presentationml.presentation	100 MB
PDF	.pdf	application/pdf	100 MB

Formatos de imagem

Tipo de imagem	Extensão	MIMETipo	Tamanho máx.
JPEG	.jpeg	image/jpeg	5 MB
PNG	.png	image/png	5 MB

Formatos de adesivos

Tipo de adesivo	Extensão	MIMETipo	Tamanho máx.
Adesivo animado	.webp	image/webp	500 KB
Adesivo estático	.webp	image/webp	100 KB

Formatos de vídeo

Tipo de vídeo	Extensão	MIMETipo	Tamanho máx.
3 GPP	.3gp	vídeo/3gp	16 MB
MP4Vídeo	.mp4	vídeo/mp4	16 MB

WhatsApp tipos de mensagem

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

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 um local
Contatos	Enviar um cartão de contato
Interativo	Envie uma mensagem interativa

Recursos adicionais

Para obter uma lista de objetos de WhatsApp mensagem, consulte Mensagens na WhatsApp Business Platform Cloud API Reference.

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

Antes de enviar uma mensagem, você deve ter concluído a configuração WABA e seu usuário deve ter optado por receber mensagens suas, 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 a um usuário quando uma janela de atendimento ao cliente está aberta entre você e o usuário. As mensagens modelo podem ser enviadas a um usuário 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 para WhatsApp um evento é gerado com um status de mensagem `defail`. Você deve ativar um destino de mensagem e evento para receber o status da mensagem.

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 e/ou limitações na distribuição de acordo com as leis e/ou regulamentos aplicáveis.

Tópicos

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

O exemplo a seguir mostra como usar um modelo para enviar uma mensagem ao 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.

```
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:

- Substituir *{PHONE_NUMBER}* pelo número de telefone de seus clientes.
- Substituir *{ORIGINATION_PHONE_NUMBER_ID}* com o 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 o 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 de tipos de arquivo de mídia com suporte, consulteTipos e tamanhos de arquivos de mídia suportados em WhatsApp.

1. Carregue o arquivo de mídia para um bucket do Amazon S3, 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:

- Substituir *{ORIGINATION_PHONE_NUMBER_ID}* com o ID do seu número de telefone.
- Substituir *{BUCKET}* pelo nome do bucket do Amazon S3.
- Substituir *{MEDIA_FILE}* 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 campo de cabeçalhos. 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
```

No comando anterior, faça o seguinte:

- Substituir *{PHONE_NUMBER}* pelo número de telefone de seus clientes.
- Substituir *{ORIGINATION_PHONE_NUMBER_ID}* com o ID do seu número de telefone.
- Substituir *{MEDIA_ID}* pelo ID da mídia retornado 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 WhatsApp seu bucket do Amazon S3.

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

No comando anterior, faça o seguinte:

- Substituir *{ORIGINATION_PHONE_NUMBER_ID}* com o ID do seu número de telefone.
- Substituir *{MEDIA_ID}* com o ID da mídia.

Respondendo a uma mensagem recebida no AWS End User Messaging Social

Antes de receber uma mensagem de texto ou de mídia, você deve ter concluído a configuração WABA e o destino do evento. Quando você recebe uma mensagem, um evento é salvo no SNS tópico Amazon de destino do evento. Você precisa se inscrever no endpoint de SNS tópicos da Amazon para receber uma notificação.

Para obter um exemplo de evento de uma mensagem de mídia recebida, consulteExemplo WhatsApp JSON de recebimento de 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 arquivo de mídia com suporte, consulteTipos e tamanhos de arquivos de mídia suportados em WhatsApp.

> **Important**
>
> Para receber mensagens recebidas, você deve ter os destinos de eventos habilitados para oWABA, consulteAdicionar um destino de mensagem e evento ao AWS End User Messaging Social.

Exemplo de alteração do status de uma mensagem para lida com 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:

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

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:

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

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

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

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

No comando anterior, faça o seguinte:

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

Exemplo de resposta a uma mensagem com 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

Você deve ter configurado um SNS tópico da Amazon de destino para o evento e se inscrever em um dos endpoints de tópicos para receber uma notificação de que Diego enviou uma mensagem.

Respondendo

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

   > **Note**
   >
   > Como Diego iniciou a conversa, isso não conta para as 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.

```
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 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 na mensagem recebida`wamid.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.

Noções básicas sobre os relatórios de uso e WhatsApp faturamento para o 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 AWS finais, consulte Preços de mensagens para usuários finais.

Campo	Opções	Descrição
Region code	• USE1— Região Leste dos EUA (N. 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 da 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 de dois dígitos ISO 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` , `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, potencial mente em várias etapas do processo de login (por exemplo, verificação de conta, recuperação de conta e desafios de integridade). • `Service`— Usado para resolver dúvidas de clientes. **`Conversat ionFee`** 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 mensagem modelo que você envia para o mesmo cliente é cobrada 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
```

Exemplo 1: envio de uma mensagem 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, ISO códigos de cobrança social e mapeamento de taxas de WhatsApp conversação

Padrão da África

Código de dois dígitos do país ISO	Nome do país	WhatsApp região de cobrança da conversa
AF	Afeganistão	Regiões da Ásia-Pacífico
AX	Ilhas Aleutas	Outros
AL	Albânia	Resto da Europa Central e Oriental
DZ	Argélia	África
AS	Samoa Americana	Outros
AD	Andorra	Outros
AO	Angola	África
AI	Anguila	Outros
AQ	Antártica	Outros
AG	Antígua e Barbuda	Outros
AR	Argentina	Argentina
AM	Armênia	Resto da Europa Central e Oriental
AW	Aruba	Outros
AC	Ilha Aleutas	Outros
AU	Austrália	Regiões da Ásia-Pacífico
AT	Áustria	Resto da Europa Ocidental
AZ	Azerbaijão	Resto da Europa Central e Oriental

Código de dois dígitos do país ISO	Nome do país	WhatsApp região de cobrança da conversa
BS	Bahamas	Outros
BH	Bahrein	Padrão do Oriente Médio
BD	Bangladesh	Regiões da Ásia-Pacífico
BB	Barbados	Outros
BY	Bielorrússia	Resto da Europa Central e Oriental
BE	Bélgica	Resto da Europa Ocidental
BZ	Belize	Outros
BJ	Benin	África
BM	Bermudas	Outros
BT	Butão	Outros
BO	Bolívia	Resto da América Latina
BQ	Bonaire	Outros
BA	Bósnia e Herzegovina	Outros
BW	Botsuana	África
BV	Ilha Bouvet	Outros
BR	Brasil	Brasil
IO	Território Britânico do Oceano Índico	Outros
VG	Ilhas Virgens Britânicas	Outros
BN	Brunei Darussalam	Outros

Código de dois dígitos do país ISO	Nome do país	WhatsApp região de cobrança da conversa
BG	Bulgária	Resto da Europa Central e Oriental
BF	BurkinaFaso	África
BI	Burundi	África
KG	Camboja	Regiões da Ásia-Pacífico
CM	Camarões	África
CA	Canadá	América do Norte
CV	Cabo Verde	Outros
KY	Ilhas Cayman	Outros
CF	República Centro-Africana	Outros
TD	Chade	África
CL	Chile	Chile
CN	China	Regiões da Ásia-Pacífico
CX	Ilha Christmas	Outros
CC	Ilhas Cocos (Keeling)	Outros
CO	Colômbia	Colômbia
KM	Comoros	Outros
CG	Congo	Outros
CD	Congo	África
CK	Ilhas Cook	Outros

Código de dois dígitos do país ISO	Nome do país	WhatsApp região de cobrança da conversa
CR	Costa Rica	Resto da América Latina
CI	Costa do Marfim	África
HR	Croácia	Resto da Europa Central e Oriental
CW	Curaçao	Outros
CY	Chipre	Outros
CZ	República Tcheca	Resto da Europa Central e Oriental
DK	Dinamarca	Resto da Europa Ocidental
DJ	Djibuti	Outros
DM	Dominica	Outros
DO	República Dominicana	Resto da América Latina
EC	Equador	Resto da América Latina
EG	Egito	Egito
SV	El Salvador	Resto da América Latina
GQ	Guiné Equatorial	Outros
ER	Eritreia	África
EE	Estônia	Outros
ET	Etiópia	África
FK	Ilhas Falkland	Outros
FO	Ilhas Faroe	Outros

Código de dois dígitos do país ISO	Nome do país	WhatsApp região de cobrança da conversa
FJ	Fiji	Outros
FI	Finlândia	Resto da Europa Ocidental
FR	França	França
GF	Guiana Francesa	Outros
PF	Polinésia Francesa	Outros
TF	Territórios Franceses do Sul	Outros
GA	Gabão	África
GM	Gâmbia	África
GE	Geórgia	Resto da Europa Central e Oriental
DE	Alemanha	Alemanha
GH	Gana	África
GI	Gibraltar	Outros
GR	Grécia	Resto da Europa Central e Oriental
GL	Groenlândia	Outros
GD	Granada	Outros
GP	Guadalupe	Outros
GU	Guam	Outros
GT	Guatemala	Resto da América Latina
GG	Guernsey	Outros

Código de dois dígitos do país ISO	Nome do país	WhatsApp região de cobrança da conversa
GN	Guiné	Outros
GW	Guiné-Bissau	África
GY	Guiana	Outros
HT	Haiti	Resto da América Latina
HM	Heard e McDonald Ilhas	Outros
HN	Honduras	Resto da América Latina
HK	Hong Kong	Regiões da Ásia-Pacífico
HU	Hungria	Resto da Europa Central e Oriental
IS	Islândia	Outros
IN	Índia	Índia
IN	Padrão da África	Padrão da África
ID	Indonésia	Indonésia
ID	Internacional Indonésia	Internacional Indonésia
IQ	Iraque	Padrão do Oriente Médio
IE	Irlanda	Resto da Europa Ocidental
IM	Ilha de Man	Outros
IL	Israel	Israel
IT	Itália	Itália
JM	Jamaica	Resto da América Latina

Código de dois dígitos do país ISO	Nome do país	WhatsApp região de cobrança da conversa
JP	Japão	Resto da Ásia-Pacífico
JE	Jérsei	Outros
JO	Jordânia	Padrão do Oriente Médio
KZ	Cazaquistão	Outros
KE	Quênia	África
KI	Quiribati	Outros
XK	Kosovo	Outros
KW	Kuwait	Padrão do Oriente Médio
KG	Quirguistão	Outros
LA	Laosiano PDR	Resto da Ásia-Pacífico
LV	Letônia	Resto da Europa Central e Oriental
LB	Líbano	Padrão do Oriente Médio
LS	Lesoto	África
LR	Libéria	África
LY	Líbia	África
LI	Liechtenstein	Outros
LT	Lituânia	Resto da Europa Central e Oriental
LU	Luxemburgo	Outros
MO	Macau	Outros

Código de dois dígitos do país ISO	Nome do país	WhatsApp região de cobrança da conversa
MK	Macedônia	Resto da Europa Central e Oriental
MG	Madagascar	África
MW	Malawi	África
MY	Malásia	Malásia
MV	Ilhas Maldivas	Outros
ML	Mali	África
MT	Malta	Outros
MH	Ilhas Marshall	Outros
MQ	Martinica	Outros
MR	Mauritânia	África
MU	Ilhas Maurício	Outros
YT	Mayotte	Outros
MX	México	México
FM	Micronésia	Outros
MD	Moldávia	Resto da Europa Central e Oriental
MC	Mônaco	Outros
MN	Mongólia	Resto da Ásia-Pacífico
ME	Montenegro	Outros
MS	Montserrat	Outros

Código de dois dígitos do país ISO	Nome do país	WhatsApp região de cobrança da conversa
MA	Marrocos	África
MZ	Moçambique	África
MM	Mianmar	Outros
N/D	Namíbia	África
NR	Nauru	Outros
NP	Nepal	Resto da Ásia-Pacífico
NL	Holanda	Holanda
NC	Nova Caledônia	Outros
NZ	Nova Zelândia	Resto da Ásia-Pacífico
NI	Nicarágua	Resto da América Latina
NE	Níger	África
NG	Nigéria	Nigéria
NU	Niue	Outros
NF	Ilha Norfolk	Outros
MP	Ilhas Marianas do Norte	Outros
NO	Noruega	Resto da Europa Ocidental
OM	Omã	Padrão do Oriente Médio
PK	Paquistão	Paquistão
PW	Palau	Outros
PS	Territórios palestinos	Outros

Código de dois dígitos do país ISO	Nome do país	WhatsApp região de cobrança da conversa
PA	Panamá	Resto da América Latina
PG	Papua Nova Guiné	Resto da Ásia-Pacífico
PY	Paraguai	Resto da América Latina
PE	Peru	Peru
PH	Filipinas	Resto da Ásia-Pacífico
PN	Pitcairn	Outros
PL	Polônia	Resto da Europa Central e Oriental
PT	Portugal	Resto da Europa Ocidental
PR	Porto Rico	Resto da América Latina
QA	Catar	Padrão do Oriente Médio
RE	Reunião	Outros
RO	Romênia	Resto da Europa Central e Oriental
RU	Federação Russa	Rússia
RW	Ruanda	África
SH	São Bartolomeu	Outros
KN	São Cristóvão e Nevis	Outros
LC	Santa Lúcia	Outros
PM	Saint Pierre e Miquelon	Outros
VC	São Vicente e Granadinas	Outros

Código de dois dígitos do país ISO	Nome do país	WhatsApp região de cobrança da conversa
BL	São Bartolomeu	Outros
MF	São Martinho	Outros
WS	Samoa	Outros
SM	São Marinho	Outros
ST	São Tomé e Príncipe	Outros
SA	Arábia Saudita	Arábia Saudita
SN	Senegal	África
RS	Sérvia	Resto da Europa Central e Oriental
SC	Seichelles	Outros
SL	Serra Leoa	África
SG	Cingapura	Resto da Ásia-Pacífico
SX	Sint Maarten	Outros
SK	Eslováquia	Resto da Europa Central e Oriental
SI	Eslovênia	Resto da Europa Central e Oriental
SB	Ilhas Salomão	Outros
SO	Somália	África
ZA	África do Sul	África do Sul

Código de dois dígitos do país ISO	Nome do país	WhatsApp região de cobrança da conversa
GS	Ilhas Geórgia do Sul e Sandwich do Sul	Outros
KR	Coreia do Sul	Outros
SS	Sudão do Sul	África
ES	Espanha	Espanha
LK	Sri Lanka	Resto da Ásia-Pacífico
SR	Suriname	Outros
SJ	Ilhas Svalbard e Jan Mayen	Outros
SZ	Suazilândia	África
SE	Suécia	Resto da Europa Ocidental
CH	Suíça	Resto da Europa Ocidental
TW	Taiwan	Resto da Ásia-Pacífico
TJ	Tajiquistão	Resto da Ásia-Pacífico
TZ	Tanzânia	África
TH	Tailândia	Resto da Ásia-Pacífico
TL	Timor-Leste	Outros
TG	Togo	África
TK	Toquelau	Outros
TO	Tonga	Outros
TT	Trinidad e Tobago	Outros

Código de dois dígitos do país ISO	Nome do país	WhatsApp região de cobrança da conversa
TA	Trist e uma Cunha	Outros
TN	Tunísia	África
TR	Turquia	Turquia
TM	Turcomenistão	Resto da Ásia-Pacífico
TC	Ilhas Turcas e Caicos	Outros
TV	Tuvalu	Outros
UG	Uganda	África
UA	Ucrânia	Resto da Europa Central e Oriental
AE	Emirados Árabes Unidos	Emirados Árabes Unidos
GB	Reino Unido	Reino Unido
EUA	Estados Unidos	América do Norte
UY	Uruguai	Resto da América Latina
UM	Ilhas Menores Distantes dos EUA	Outros
UZ	Uzbequistão	Resto da Ásia-Pacífico
VU	Vanuatu	Outros
VA	Padrão da Ásia-Pacífico	Outros
VE	Venezuela	Resto da América Latina
VN	Vietnã	Resto da Ásia-Pacífico
VI	Ilhas Aleutas	Outros

Código de dois dígitos do país ISO	Nome do país	WhatsApp região de cobrança da conversa
WF	Ilhas Wallis e Futuna	Outros
EH	Saara Ocidental	Outros
YE	Iêmen	Padrão do Oriente Médio
ZM	Zâmbia	África
ZW	Zimbábue	Outros

Monitorando as mensagens sociais do usuário AWS final

O monitoramento é uma parte importante para manter a confiabilidade, a disponibilidade e o desempenho do AWS End User Messaging Social e de outras AWS soluções da. AWSA fornece as seguintes ferramentas de monitoramento para observar o AWS End User Messaging Social, informar quando algo está errado e realizar ações automáticas quando apropriado:

- A Amazon CloudWatch monitora os AWS recursos da e as aplicações que você executa na 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 fazer com que o CloudWatch rastreie o CPU uso ou outras métricas das EC2 instâncias da Amazon e inicie automaticamente novas instâncias quando necessário. Para obter mais informações, consulte o Guia CloudWatch do usuário da Amazon.
- O Amazon CloudWatch Logs permite monitorar, armazenar e acessar os arquivos de log de EC2 instâncias da Amazon CloudTrail, do e de outras fontes. CloudWatch O Logs pode monitorar informações nos arquivos de log e notificar você 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 CloudTrailO captura API chamadas e eventos relacionados feitos por, ou em nome de, sua AWS conta da e entrega os arquivos de log a um bucket do Amazon S3 que você especificar. Você pode identificar quais usuários e contas chamaram a AWS, o endereço IP de origem 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.

A tabela a seguir lista as métricas e as 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 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 seu envolvimento com os clientes 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

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. A fornece os seguintes recursos para ajudar com a conformidade:

- 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 cadastrar para receber suas mensagens usando um formulário on-line, evite que scripts automatizados inscrevam pessoas sem o conhecimento delas. Além disso, limite 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 regulamentações 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. Quando você precisar de ajuda WhatsApp, entre em contato com seu administrador:

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 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

Usar credenciais temporárias para o FIS Se você envia mensagens na hora do jantar ou no meio da noite, há uma boa chance de que seus clientes cancelarão a inscrição de suas listas para não serem mais perturbados. Talvez você queira evitar o envio de WhatsApp mensagens quando seus clientes não conseguem responder a elas imediatamente.

Segurança nas mensagens sociais do usuário AWS final

A segurança da nuvem na AWS é a nossa maior prioridade. Como AWS cliente da, você se beneficiará de datacenters e arquiteturas de rede criados para atender aos requisitos das empresas com as maiores exigências de segurança.

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

- Segurança da nuvem: a AWS é responsável por proteger a infraestrutura que executa AWS serviços da no Nuvem AWS. AWS A AWS também fornece serviços que você pode usar com segurança. Auditores de terceiros testam e verificam regularmente a eficácia da nossa segurança como parte dos Programas de conformidade da Programas de conformidade da Programas de AWS conformidade da Programas de de da. Para saber mais sobre os programas de conformidade que se aplicam ao AWS End User Messaging Social, consulte AWS Serviços da em escopo por programa de conformidade AWS .
- Segurança na nuvem: sua responsabilidade é determinada pelo AWS serviço da 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 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. Saiba também como usar outros AWS serviços da que ajudam você a monitorar e proteger os recursos sociais de mensagens do usuário AWS final.

Tópicos

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 nesse modelo, a AWS é responsável por proteger a infraestrutura global que executa toda a Nuvem AWS. Você é responsável por manter o controle sobre seu 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 a Privacidade de dados FAQ. Para obter informações sobre proteção de dados na Europa, consulte o Modelo de Responsabilidade AWS Compartilhada e GDPR a postagem no blog AWS de segurança.

Para fins de proteção de dados, recomendamos que você proteja Conta da AWS as credenciais da e configure as contas de usuário individuais com o AWS IAM Identity Center ou o 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 a autenticação multifator (MFAMFA) com cada conta.
- UseSSL/TLSpara se comunicar com AWS os recursos. Exigimos TLS TLS 1.2 e recomendamos TLS TLS 1.2.
- Configure o registro em log das atividades da API API e do usuário com o 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 as soluções de AWS criptografia, juntamente com todos os controles de segurança padrão em 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 FIPS 140-3 módulos criptográficos validados ao acessar a AWS por meio de uma interface de linha de comando ou umaAPI, use um endpoint. FIPS Para obter mais informações sobre os FIPS endpoints disponíveis, consulte Federal Information Processing Standard (FIPS) 140-3.

É altamente recomendável que nunca sejam colocadas informações de identificação confidenciais, como endereços de e-mail dos seus clientes, em marcações 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 consoleAPI,, AWS CLI, ou AWS SDKs. Quaisquer dados inseridos em tags ou 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, recomendemos fortemente que não sejam incluídas informações de credenciais no URL para validar a solicitação a esse 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 do usuário final Os dados sociais são criptografados em trânsito e em repouso dentro do AWS limite. Quando você envia dados para o AWS End User Messaging Social, ele criptografa os dados conforme os recebe 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 os dados de configuração, os dados de registro e todos os dados que você adicionar ao AWS End User Messaging Social. Para criptografar os dados, o AWS End User Messaging Social usa chaves internas do 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 recurso Social de mensagens de usuário final do HTTPS e o Transport Layer Security (TLS) 1.2 para se comunicar com clientes, aplicativos e o 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 AWS SMS recursos usando o console, um ou o AWS SDK AWS Command Line Interface, todas as comunicações são protegidas usando HTTPS e TLS 1.2.

Gerenciamento de chaves

Para criptografar os dados, o AWS End User Messaging Social usa AWS KMS chaves internas do serviço e que mantém em seu nome. Nós mudamos essas chaves regularmente. Não é possível provisionar e usar as suas próprias AWS KMS ou outras chaves para criptografar os dados armazenados 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 clientes e aplicativos on-premises, e entre o AWS End User Messaging Social e outros AWS recursos no mesmo. Região da AWS Os seguintes atributos e práticas podem ajudar você a proteger a privacidade de tráfego entre redes para usuários AWS finais do End User Messaging Social.

Tráfego entre clientes do AWS SMS e no local e os aplicativos

Para estabelecer uma conexão privada entre o AWS End User Messaging Social e clientes e aplicativos na rede on-premises, é possível usar o 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 Messaging Social por meio do PublishedAPIs, recomendamos que você cumpra os requisitos do AWS End Messaging Social para API chamadas. AWS O End User Messaging Social requer que os clientes usem Transport Layer Security (TLS) 1.2 ou posterior. Os clientes também devem oferecer suporte a pacotes de criptografia com Perfect Forward Secrecy (PFS), como Ephemeral Diffie-Hellman () ou Ephemeral Elliptic Curve Diffie-Hellman (). DHE ECDHE 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 AWS Identity and Access Management (IAM) da AWS conta da conta da. 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 AWS o Cost Management

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. IAMos administradores controlam quem pode ser autenticado (conectado) e autorizado (ter permissões) a usar os recursos sociais do AWS End User Messaging. IAMO IAM é um serviço da AWS service (Serviço da AWS) que pode ser usado sem custo adicional.

Tópicos

Público

O uso do AWS Identity and Access Management (IAM) varia dependendo do trabalho que for realizado no AWS End User Messaging Social.

Usuário do serviço — Se você usar o serviço social AWS End User Messaging para fazer o trabalho, o administrador fornecerá as credenciais e as permissões necessárias. À medida que você usar mais recursos sociais de mensagens do usuário AWS final para fazer seu trabalho, poderá precisar de permissões adicionais. Entender como o acesso é gerenciado pode ajudar você a solicitar as permissões corretas ao seu administrador. Se não for possível acessar um atributo no AWS End User Messaging Social, consulteSolução de problemas de mensagens de usuário AWS final: identidade social e acesso.

Administrador do serviço — Se você for o responsável pelos recursos do AWS End Messaging Social na sua empresa, provavelmente terá acesso total ao AWS End Messaging Social. É sua função determinar quais recursos e funcionalidades do AWS End User Messaging Social os usuários do serviço devem acessar. Assim, é necessário enviar solicitações ao IAM administrador do para alterar

as permissões dos usuários de seu serviço. Revise as informações nesta página para entender os conceitos básicos doIAM. Para saber mais sobre como a empresa pode usar o IAM AWS End User Messaging Social, consulteComo o AWS End User Messaging Social funciona com IAM.

IAMadministrador — Se você for um IAM administrador, talvez queira saber detalhes sobre como escrever políticas para gerenciar o acesso ao AWS End User Messaging Social. Para visualizar exemplos de políticas baseadas em identidade social do usuário AWS final que podem ser usadas noIAM, consulte. Exemplos de políticas baseadas em identidade para o AWS Cost Management

Autenticando com identidades

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

Você pode fazer login na AWS como uma identidade federada usando credenciais fornecidas por uma fonte de identidades. AWS IAM Identity Center Os usuários do (IAMIdentity Center), a autenticação única da empresa e as suas credenciais do Google ou do Facebook são exemplos de identidades federadas. Quando você faz login como uma identidade federada, o administrador já configurou anteriormente a federação de identidades usando perfis doIAM. Quando você acessa a AWS usando a AWS, está indiretamente assumindo um perfil.

A depender do tipo de usuário, você pode fazer login 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 a AWS programaticamente, a AWS fornecerá um kit de desenvolvimento de software (SDK) e uma interface de linha de comando (CLI) para você assinar criptograficamente as solicitações usando as suas credenciais. Se você não utilizar AWS as ferramentas da, você deverá assinar a solicitação por conta própria. Para obter mais informações sobre o uso do método recomendado para designar solicitações por conta própria, consulte Assinar AWS API solicitações no Guia do IAM usuário do.

Independente do método de autenticação usado, também pode ser exigido que você forneça informações adicionais de segurança. Por exemplo, a AWS recomenda o uso da autenticação multifator (MFA) para aumentar a segurança da conta. Para saber mais, consulte Autenticação multifator no Guia AWS IAM Identity Center do usuário e Uso da autenticação multifator (MFA) AWS no Guia do IAMusuário.

Conta da AWS usuário root

Ao criar uma Conta da AWS, você começa com uma identidade de login que tenha acesso completo a todos os Serviços da AWS e recursos na conta. Essa identidade é denominada usuário Conta da AWS raiz da e é acessada pelo 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 IAM usuário do.

Identidade federada

Como prática recomendada, exija que os usuários, inclusive os que precisam de acesso de administrador, utilizem a federação com um provedor de identidades para acessar os Serviços da AWS usando credenciais temporárias.

Identidade federada é um usuário de seu diretório de usuários corporativos, um provedor de identidades da Web, o AWS Directory Service, o diretório do Identity Center ou qualquer usuário que acesse os usando credenciais fornecidas Serviços da AWS por meio de uma fonte de identidade. Quando as identidades federadas acessam Contas da AWS, elas assumem perfis que fornecem credenciais temporárias.

Para o gerenciamento de acesso centralizado, recomendamos usar o AWS IAM Identity Center. Você pode criar usuários e grupos no IAM Identity Center ou conectar-se e sincronizar com um conjunto de usuários e grupos em sua própria fonte de identidade para uso em todas as suas Contas da AWS e aplicações. Para obter informações sobre o IAM Identity Center, consulte O que é o IAM Identity Center? no Guia do AWS IAM Identity Center usuário.

Grupos e usuários do IAM

Um IAMusuário é uma identidade dentro da sua Conta da AWS que tem permissões específicas para uma única pessoa ou aplicativo. Sempre que possível, recomendamos depender de credenciais temporárias em vez de criar IAM usuários 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 IAM usuários, recomendamos alternar as chaves de acesso. Para obter mais informações, consulte Alterne as chaves de acesso regularmente para casos de uso que exigem credenciais de longo prazo no Guia IAM do usuário do.

Um IAMgrupo é uma identidade que especifica uma coleção de IAM usuários. 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 denominado IAMAdminse atribuir a esse grupo permissões para administrar IAM recursos do.

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 Quando criar um IAM usuário (em vez de uma função) no Guia do IAM usuário.

IAMfunções

Uma IAMfunção é uma identidade dentro da sua Conta da AWS que tem permissões específicas. Ela é semelhante a um IAM usuário do, mas não está associada a uma pessoa específica. É possível presumir IAM temporariamente um perfil no AWS Management Console alternando perfis. Você pode assumir uma função chamando uma AWS API operação AWS CLI or ou usando uma personalizadaURL. Para obter mais informações sobre métodos de uso de funções, consulte Métodos para assumir uma função no Guia IAM do usuário.

IAMAs funções do com credenciais temporária são úteis nas seguintes situações:

- Acesso de usuário federado: para atribuir permissões a identidades federadas, você pode 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 pelo mesmo. Para obter informações sobre funções para federação, consulte Criação de uma função para um provedor de identidade terceirizado no Guia IAM do usuário. Se você usar o IAM Identity Center, configure um conjunto de permissões. Para controlar o que suas identidades podem acessar após a autenticação, o IAM Identity Center correlaciona o conjunto de permissões a um perfil no. IAM Para obter informações sobre conjuntos de permissões, consulte Conjuntos de Permissões no Manual do Usuário do AWS IAM Identity Center .
- Permissões temporárias IAM para usuários: um IAM usuário ou um perfil pode IAM assumir um perfil para obter temporariamente permissões diferentes para uma tarefa específica.
- Acesso entre contas: é possível usar uma IAM função do para permitir que alguém (um principal confiável) em outra conta acesse recursos em sua conta. Os perfis são a principal forma de conceder acesso entre contas. No entanto Serviços da AWS, alguns permitem que você anexe uma política diretamente a um recurso (em vez de usar uma função como proxy). Para saber a diferença entre perfis e políticas baseadas em recurso para acesso entre contas, consulte Acesso a recursos entre contas IAM no Guia do usuário doIAM.

- Acesso entre serviços: alguns Serviços da AWS usam atributos em outros Serviços da AWS. Por exemplo, quando você faz uma chamada em um serviço, é comum que esse serviço execute aplicações na Amazon EC2 ou armazene objetos no Amazon S3. Um serviço pode fazer isso usando as permissões do principal de chamada, usando um perfil de serviço ou um perfil vinculado a serviço.
  - Sessões de acesso direto (FAS): qualquer pessoa que utilizar uma função ou IAM usuário para realizar ações na AWSé considerada uma entidade principal do. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. FASusa as permissões da entidade principal que chama um AWS service (Serviço da AWS), combinadas às permissões do solicitante, AWS service (Serviço da AWS) para realizar solicitações para serviços downstream. FASas solicitações só são feitas quando um serviço recebe uma solicitação que exige interações com outros Serviços da AWS ou com recursos para serem concluídas. Nesse caso, você precisa ter permissões para executar ambas as ações. Para obter detalhes da política ao fazer FAS solicitações, consulte Encaminhamento de sessões de acesso.
  - Função de serviço: uma função de serviço é uma IAMfunção que um serviço assume para realizar ações em seu nome. Um IAM administrador do pode criar, modificar e excluir um perfil de serviço a partir doIAM. Para obter mais informações, consulte Criação de uma função para delegar permissões a uma AWS service (Serviço da AWS) no Guia do IAM usuário.
  - Função vinculada ao serviço: uma função vinculada ao serviço é um tipo de função de serviço vinculada a uma. AWS service (Serviço da AWS) O serviço pode presumir a função de executar uma ação em seu nome. Funções vinculadas ao serviço aparecem em sua Conta da AWS e são de propriedade do serviço. Um IAM administrador do pode visualizar, mas não pode editar as permissões para funções vinculadas ao serviço.
- Aplicativos em execução na Amazon EC2 — Você pode usar uma IAM função para gerenciar credenciais temporárias para aplicativos que estão sendo executados em uma EC2 instância e fazendo AWS CLI AWS API solicitações. É preferível fazer isso a armazenar chaves de acesso na EC2 instância do Amazon EC2. Para atribuir um AWS perfil da a uma EC2 instância do e disponibilizá-la para todas as suas aplicações, crie um perfil de instância que esteja anexado a ela. Um perfil da instância contém a função e permite que programas que estão em execução na EC2 instância obtenham credenciais temporárias. Para obter mais informações, consulte Como usar uma IAM função para conceder permissões a aplicativos executados em EC2 instâncias da Amazon no Guia IAM do usuário.

Para saber se usar IAM funções ou IAM usuários, consulte Quando criar uma IAM função (em vez de um usuário) no Guia do IAM usuário.

Gerenciando acesso usando políticas

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

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

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

IAMAs políticas do 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 do AWS Management Console AWS CLI, do ou do AWS API.

Políticas baseadas em identidade

As políticas baseadas em identidade são documentos de políticas de JSON permissões que você pode anexar a uma identidade, como um IAM usuário, grupo de usuários ou função. 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 Criação de IAM políticas no Guia do IAMusuário.

As políticas baseadas em identidade podem ser categorizadas ainda adicionalmente 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 independentes que podem ser anexadas a vários usuários, grupos e funções na. Conta da AWS As políticas gerenciadas incluem políticas AWS gerenciadas pela 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 IAM do usuário do.

Políticas baseadas no recurso

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

Políticas baseadas em recursos são políticas em linha localizadas nesse serviço. Não é possível usar as políticas AWS gerenciadas da IAM no em uma política baseada em recursos.

Listas de controle de acesso (ACLsACLs)

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

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

Outros tipos de política

AWS A oferece compatibilidade com tipos de política 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 atributo avançado no qual você define o máximo de permissões que uma política baseada em identidade pode conceder a uma IAM entidade (IAMusuário ou função). 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 IAM entidades do no Guia do IAM usuário do.
- Políticas de controle de serviço (SCPs): SCPs são JSON políticas que especificam o máximo de permissões para uma organização ou unidade organizacional (UO) em AWS Organizations.

AWS Organizations O 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 contas. Os SCP limites de permissões para entidades em contas-membro, incluindo cada Usuário raiz da conta da AWS. Para obter mais informações sobre Organizations eSCPs, consulte Políticas de controle de serviços 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 atributo. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações, consulte Políticas de sessão no Guia IAM do usuário.

Vários tipos de política

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

Como o AWS End User Messaging Social funciona com IAM

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

IAMrecursos que você pode usar com o AWS End User Messaging Social

IAMrecurso	AWS Suporte social de mensagens para o usuário final
Políticas baseadas em identidade	Sim
Políticas baseadas em recursos	Não
Ações das políticas	Sim

IAMrecurso	AWS Suporte social de mensagens para o usuário final
Atributos de políticas	Sim
Chaves de condição de políticas	Sim
ACLs	Não
ABAC(tags nas políticas)	Parcial
Credenciais temporárias	Sim
Permissões de entidade principal	Sim
Perfis de serviço	Sim
Funções vinculadas a serviço	Sim

Para ter uma visão geral de como os AWS serviços sociais de mensagens para usuários AWS finais e outros funcionam com a maioria dos IAM recursos, consulte AWS os serviços que funcionam com IAM no Guia do IAM usuário.

Políticas baseadas em identidade para o AWS FIS

Compatível com políticas baseadas em identidade: Sim

As políticas baseadas em identidade são documentos de políticas de JSON permissões que você pode anexar a uma identidade, como um IAM usuário, grupo de usuários ou função. 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 Criação de IAM políticas no Guia do IAMusuário.

Com as políticas IAM baseadas em identidade, é possível especificar ações ou recursos permitidos ou negados, bem 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 você pode usar em uma JSON política, consulte a referência IAM JSON de elementos de política no Guia IAM do usuário.

Exemplos de políticas baseadas em identidade para o AWS Cost Management

Para ver exemplos de políticas baseadas em identidade social do AWS End User Messaging, consulte. Exemplos de políticas baseadas em identidade para o AWS Cost Management

Políticas baseadas em identidade para AWS o FIS

Suporte a políticas baseadas em recursos: não

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

Para permitir o acesso entre contas, você pode especificar uma conta inteira ou IAM as entidades do em outra conta como o principal em uma política baseada em atributo. Adicionar uma entidade principal entre contas à política baseada em recurso é apenas metade da tarefa de estabelecimento da relação de confiança. Quando a entidade principal e o recurso estão em diferentes Contas da AWS, um IAM administrador da conta confiável também deve conceder à entidade principal (usuário ou função) permissão 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. Para obter mais informações, consulte Acesso a recursos entre contas IAM no Guia do IAM usuário.

Ações de política para mensagens sociais de usuário AWS final

Compatível com ações de políticas: Sim

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

O `Action` elemento de uma JSON política descreve as ações que você pode usar para permitir ou negar acesso em uma política. As ações de política geralmente têm o mesmo nome que a AWS API operação associada. Existem algumas exceções, como ações somente de permissão, que não

têm uma operação correspondente. API 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 instrução, separe-as com vírgulas.

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

Para ver exemplos de políticas baseadas em identidade social do AWS End User Messaging, consulte. Exemplos de políticas baseadas em identidade para o AWS Cost Management

Recursos de política para mensagens sociais para usuários AWS finais

Compatível com recursos de políticas: Sim

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

O elemento `Resource` JSON de política 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 seusARNs, consulte Recursos definidos pelo AWS End User Messaging Social na Referência de Autorização do Serviço. Para saber com quais ações você pode especificar cada recurso, consulte Ações definidas pelo AWS End User Messaging Social. ARN

Para ver exemplos de políticas baseadas em identidade social do AWS End User Messaging, consulte. Exemplos de políticas baseadas em identidade para o AWS Cost Management

Chaves de condição de AWS política para o FIS

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

Os administradores podem usar AWS JSON as políticas para especificar quem tem acesso a 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 `Condition` em uma instrução ou várias chaves em um único `Condition` elemento, a AWS os avaliará usando uma operação lógica `AND`. Se você especificar vários valores para uma única chave de condição, AWS a avaliará a condição usando uma `OR` 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, você pode conceder a um IAM usuário do permissão para acessar um recurso somente se ele estiver marcado com seu nome de IAM usuário do. Para obter mais informações, consulte elementos de IAM política: variáveis e tags no Guia IAM do usuário.

AWS A oferece suporte a chaves de condição globais e chaves de condição específicas do serviço. Para consultar todas as chaves de condição AWS globais da, consulte Chaves de contexto de condição AWS globais da no Guia IAM do usuário do.

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 é possível usar uma chave de condição, consulte Ações definidas pelo AWS End User Messaging Social.

Para ver exemplos de políticas baseadas em identidade social do AWS End User Messaging, consulte. Exemplos de políticas baseadas em identidade para o AWS Cost Management

ACLsnas redes sociais de mensagens do usuário AWS final

SuportesACLs: Não

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

ABACcom mensagens sociais para usuários AWS finais

Suportes ABAC (tags nas políticas): Parciais

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

ABACé 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 oferecer suporte às três chaves de condição para cada tipo de recurso, o valor será Sim para o serviço. Se um serviço oferecer suporte às três chaves de condição somente para alguns tipos de recursos, o valor será Parcial

Para obter mais informações sobreABAC, consulte O que éABAC? no Guia do IAM usuário. Para ver um tutorial com etapas de configuraçãoABAC, consulte Usar controle de acesso baseado em atributos (ABAC) no Guia do IAMusuário.

Usar credenciais temporárias com AWS o FIS

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 esse trabalho IAM no Guia do IAM usuário.

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

Você pode criar manualmente credenciais temporárias usando o AWS CLI ou AWS API. Em seguida, você pode usar essas credenciais temporárias para acessar AWS. AWS A 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 emIAM.

Permissões de entidade principal entre serviços para AWS o Cost Management

Suporte ao recurso de encaminhamento de sessões de acesso (FASFAS):

Quando você usa um IAM usuário ou uma função para executar ações na AWS, você é considerado um principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. FASusa as permissões da entidade principal que chama um AWS service (Serviço da AWS), combinadas às permissões do solicitante, AWS service (Serviço da AWS) para realizar solicitações para serviços downstream. FASas solicitações só são feitas quando um serviço recebe uma solicitação que exige interações com outros Serviços da AWS ou com recursos para serem concluídas. Nesse caso, você precisa ter permissões para executar ambas as ações. Para obter detalhes da política ao fazer FAS solicitações, consulte Encaminhamento de sessões de acesso.

Funções de serviço para mensagens sociais de usuário AWS final

Compatível com perfis de serviço: Sim

A função de serviço é uma IAMfunção que um serviço assume para executar ações em seu nome. Um IAM administrador do pode criar, modificar e excluir um perfil de serviço a partir doIAM. Para obter mais informações, consulte Criação de uma função para delegar permissões a uma AWS service (Serviço da AWS) no Guia do IAM usuário.

> **Warning**
>
> Alterar as permissões de um perfil de serviço pode prejudicar a funcionalidade do AWS End User Messaging Social. Só edite os perfis de serviço quando AWS o End User Messaging Social orientar você a fazê-lo.

Funções vinculadas a serviços para mensagens sociais de usuário AWS final

Suporte a perfis vinculados a serviços: sim

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

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

Exemplos de políticas baseadas em identidade para o AWS Cost Management

Por padrão, usuários e funções não têm permissão para criar ou modificar recursos sociais de mensagens de usuário AWS final. Eles também não podem realizar tarefas usando o AWS Management Console, AWS Command Line Interface (AWS CLI) ou AWS API. Para conceder aos usuários permissões para executar ações nos recursos de que eles precisam, um IAM administrador do pode criar IAM políticas do. O administrador pode então adicionar as IAM políticas do às funções, e os usuários podem assumir as funções.

Para saber como criar uma política IAM baseada em identidade usando esses exemplos de documentos de JSON política, consulte Criação de IAM políticas no Guia do IAMusuário.

Para obter informações 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 do serviço.

Tópicos

Melhores práticas de política

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

- Comece com as políticas AWS gerenciadas pela e avance para as permissões de privilégio mínimo —- para começar a conceder permissões a seus usuários e workloads, use as políticas AWS gerenciadas pela, 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 da específicas para seus casos de uso. Para obter mais informações, consulte políticas AWS gerenciadas ou políticas AWS gerenciadas para funções de trabalho no Guia IAM do usuário.
- Aplique permissões de privilégio mínimo: ao definir permissões com as IAM políticas do, conceda apenas as permissões necessárias para executar uma tarefa. Você faz isso definindo as ações que podem ser executadas em atributos específicos sob condições específicas, também conhecidas como permissões de privilégio mínimo. Para obter mais informações sobre IAM como usar para aplicar permissões, consulte Políticas e permissões IAM no Guia IAM do usuário.
- Use condições nas IAM políticas do 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 usandoSSL. Você também pode usar condições para conceder acesso a ações de serviço, se elas forem usadas por meio de um específico AWS service (Serviço da AWS), como o AWS CloudFormation. Para obter mais informações, consulte Elementos IAM JSON da política: Condição no Guia IAM do usuário.
- Use o IAM Access Analyzer para validar as IAM políticas do a fim de garantir permissões seguras e funcionais: o IAM Access Analyzer valida as políticas novas e existentes para que elas sigam a linguagem da IAM política (JSON) e as práticas recomendadas. IAM IAMO Access Analyzer oferece mais de 100 verificações de política e recomendações acionáveis para ajudar você a criar

políticas seguras e funcionais. Para obter mais informações, consulte Validação da política do IAM Access Analyzer no Guia do IAM Usuário.

- Exigir autenticação multifator (MFA) —- se houver um cenário que exija IAM usuários ou um usuário raiz em sua Conta da AWS, ative a MFA para obter segurança adicional. Para exigir MFA quando API as operações forem chamadas, adicione MFA condições às suas políticas. Para obter mais informações, consulte Configurando o API acesso MFA protegido no Guia do IAMusuário.

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

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 precisam autorizar você a listar e visualizar detalhes sobre os recursos sociais de mensagens do usuário AWS final na sua Conta da AWS. Se você criar uma política baseada em identidade que seja mais restritiva do que as permissões mínimas necessárias, o console não funcionará como pretendido para entidades (usuários ou perfis) com essa política.

Não é necessário conceder permissões mínimas do console para usuários que fazem chamadas somente ao AWS CLI ou ao AWS API. Em vez disso, permita o acesso somente às ações que correspondem à API operação que estão tentando executar.

Para garantir que os usuários e os perfis ainda possam usar o console do AWS End User Messaging, anexe também o AWS End Messaging Social *ConsoleAccess* ou a política *ReadOnly* AWS gerenciada da às entidades. Para obter mais informações, consulte Adicionar permissões a um usuário no Guia do IAM usuário.

Permitir que usuários visualizem suas próprias permissões

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

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

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

AWS 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 pela do que escrever políticas por conta própria. É necessário tempo e experiência para criar políticas gerenciadas pelo IAM cliente que fornecem à sua equipe apenas as permissões de que precisam. Para começar rapidamente, você pode usar nossas políticas AWS gerenciadas pela. 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 IAM do usuário.

AWS Os serviços da mantêm e atualizam políticas AWS gerenciadas pela. Não é possível alterar as permissões em políticas AWS gerenciadas pela. 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 permissões de uma política AWS gerenciada pela, portanto, as atualizações de políticas não suspendem suas permissões existentes.

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

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

Visualize detalhes sobre atualizações em políticas AWS gerenciadas pela para o AWS End User Messaging Social desde que esse serviço começou a rastrear essas alterações. Para receber alertas automáticos sobre alterações feitas nesta página, inscreva-se no RSS feed na págin Document History (Histórico de documentos sociais) do AWS End User.

Alteração	Descrição	Data
AWS O End User Messaging Social começou a monitorar as alterações	AWS O End User Messaging Social começou a monitorar alterações em políticas AWS gerenciadas pela.	26 de setembro 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. IAM

Tópicos

Não tenho autorização para executar uma ação AWS no Amazon IVS

Se você receber uma mensagem de erro informando que não tem autorização para executar uma ação, é preciso atualizar suas políticas para permitir que você realize a ação.

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

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

Não tenho autorização para executar uma ação no PassRole

Se você receber uma mensagem de erro informando que não tem autorização para executar a `iam:PassRole` ação, as suas políticas deverão 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 o serviço, em vez de criar uma nova função de serviço ou 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 IAM usuário do nome `marymajor` tenta usar o console para executar 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 você precisar de ajuda, entre em contato com seu AWS administrador. Seu administrador é a pessoa que forneceu suas credenciais de login.

Desejo permitir que pessoas fora da minha acessem meus Conta da AWS recursos sociais do AWS End User Messaging

Você pode criar um perfil que os usuários de outras contas ou pessoas fora da sua organização podem usar para acessar seus recursos. Você pode 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 IAM.
- Para saber como conceder acesso a seus recursos em Contas da AWS de sua propriedade, consulte Conceder acesso a um IAM usuário em outra Conta da AWS de sua propriedade no Guia do IAM usuário do.
- Para saber como conceder acesso a seus recursos em de terceiros Contas da AWS, consulte Conceder acesso Contas da AWS a de terceiros no Guia do IAM usuário do.
- Para saber como conceder acesso por meio da federação de identidades, consulte Conceder acesso a usuários autenticados externamente (federação de identidades) no Guia IAM do usuário do.
- Para saber a diferença entre perfis e políticas baseadas em recurso para acesso entre contas, consulte Acesso a recursos entre contas IAM no Guia do usuário doIAM.

Validação de conformidade para mensagens sociais de usuário AWS final

Para saber se um AWS service (Serviço da AWS) está no escopo de programas específicos de conformidade, consulte Serviços da AWS no escopo por programa de conformidade Serviços da AWS de conformidade e selecione o programa de conformidade do seu interesse. Para obter informações gerais, consulte Programas de AWS conformidade Programas AWS de .

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

Sua responsabilidade de conformidade ao usar o Serviços da AWS é determinada pela confidencialidade dos dados, pelos objetivos de conformidade da empresa e pelos regulamentos e leis aplicáveis. AWS A fornece os seguintes recursos para ajudar com a conformidade:

- Guias de referência rápida de conformidade e segurança: esses guias de implantação discutem considerações sobre arquitetura e fornecem etapas para implantar ambientes de linha de base focados em segurança e conformidade na AWS concentrados em conformidade e segurança na.
- Architecting for HIPAA Security and Compliance on Amazon Web Services (Arquitetura para segurança e conformidade na Amazon Web Services): esse artigo técnico descreve como as empresas podem usar AWS a para criar aplicações elegíveisHIPAA.

  > **Note**
  >
  > Nem todos Serviços da AWS são HIPAA elegíveis. Para obter mais informações, consulte a Referência dos serviços HIPAA qualificados.

- AWS Recursos de de conformidade da: essa coleção de manuais e guias pode ser aplicada ao seu setor e seu local.
- AWS Guias de conformidade do cliente da: entenda o modelo de responsabilidade compartilhada sob a ótica da conformidade. Os guias resumem as práticas recomendadas para proteção de 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 or de Cartões de Pagamento (PCI) e a Organização Internacional de Padronização ()). ISO

- Avaliar recursos com regras no Guia do AWS Config desenvolvedor do: o AWS Config serviço avalia como as configurações de recursos estão em conformidade com práticas internas, diretrizes do setor e regulamentos.
- 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: este AWS service (Serviço da AWS) detecta possíveis ameaças às suas Contas da AWS, workloads, contêineres e dados ao monitorar o ambiente em busca de atividades suspeitas e maliciosas. GuardDuty pode ajudar você a atender a vários requisitos de conformidade PCIDSS, como atender aos requisitos de detecção de intrusões requeridos por determinadas estruturas de conformidade.
- AWS Audit Manager: esse AWS service (Serviço da AWS) ajuda a auditar continuamente seu AWS uso da para simplificar a forma como você gerencia os riscos e a conformidade com regulamentos e padrões do setor.

Resiliência nas mensagens AWS sociais do usuário final

A infraestrutura AWS global da é criada com base em Regiões da AWS e zonas de disponibilidade. Regiões da AWS As fornecem várias zonas de disponibilidade separadas e isoladas fisicamente, que são conectadas com baixa latência, throughputs elevadas e redes altamente redundantes. Com as zonas de disponibilidade, é possível projetar e operar aplicativos 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 centers tradicionais.

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

Além da infraestrutura AWS global da, o AWS End User Messaging Social oferece vários recursos para ajudar a atender às necessidades de resiliência de dados 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 de segurança de rede AWS global da que estão descritos no whitepaper Amazon Web Services: Overview of Security Processes.

Você usa API chamadas AWS publicadas para acessar o AWS End User Messaging Social por meio da rede. Os clientes devem ser compatíveis com o Transport Layer Security (TLSTLS) 1.0 ou posterior. A maioria das políticas é TLS compatível com o TLS. Os clientes também devem oferecer suporte a pacotes de criptografia com Perfect Forward Secrecy (PFS) como (Ephemeral Diffie-Hellman) ou DHE (Elliptic Curve Diffie-Hellman). ECDHE 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 IAM entidade principal do. Ou você pode 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. Na AWS, a personificação entre serviços pode resultar no problema do 'confused deputy'. 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 confused deputy é usar a chave de contexto ARN de condição `aws:SourceArn` global com o recurso completo. Se você não souber a totalidade ARN do recurso ou estiver especificando vários recursos, use a chave de condição de contexto `aws:SourceArn` global com caracteres curinga (*) para as partes desconhecidas do. ARN Por exemplo, `arn:aws:social-messaging:*:123456789012:*`.

Se o `aws:SourceArn` valor não contiver o ID da conta, como um bucket do Amazon S3ARN, 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 é possível usar as chaves `aws:SourceArn` de contexto de condição `aws:SourceAccount` globais da no Social Messaging para evitar o problema confused deputy.

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

Melhores práticas de segurança

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

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

Usar funções vinculadas ao serviço para o CodeStar AWS Notifications

AWS O End User Messaging Social usa AWS Identity and Access Management (IAM) funções vinculadas ao serviço. Um perfil vinculado ao serviço é um tipo exclusivo de perfil IAM vinculado diretamente ao AWS End User Messaging Social. As funções vinculadas a serviços são predefinidas pelo AWS End User Messaging Social e incluem todas as permissões que o serviço requer para chamar outros AWS serviços da em seu nome.

Um perfil vinculado ao serviço facilita a configuração do AWS End User Messaging Social porque você não precisa adicionar as permissões necessárias manualmente. AWS O End User Messaging Social define as permissões dos perfis vinculados ao serviço e, a não ser que esteja definido de outra forma, somente o AWS End User Messaging Social pode assumir os perfis. As permissões definidas incluem a política de confiança e a política de permissões, e essa política não pode ser anexada a nenhuma outra IAM entidade do.

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, pois você não pode remover por engano as permissões para acessar os recursos.

Para obter informações sobre outros serviços que oferecem suporte às funções vinculadas a serviços, consulte AWS serviços da compatíveis com IAM e procure os serviços que apresentam

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

Permissões de função vinculada ao serviço para o CodeStar AWS Notifications

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 AWSServiceRoleForSocialMessaging vinculada ao serviço confia nos seguintes serviços para assumir a função:

- `social-messaging.amazonaws.com`

A política de permissões da função denominada AWSSocialMessagingServiceRolePolicy 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 Permissões de funções vinculadas ao serviço no Guia do IAMusuário.

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

Criação de funções vinculadas ao serviço para o CodeStar AWS Notifications

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

Editar uma função vinculada ao serviço para o CodeStar AWS Notifications

AWS O End User Messaging Social não permite editar a função AWSServiceRoleForSocialMessaging 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, você poderá editar a descrição da função usando o IAMIAM. Para obter mais informações, consulte Edição de uma função vinculada ao serviço no Guia do IAMusuário.

Excluir uma função vinculada ao serviço para o CodeStar AWS Notifications

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 sua função vinculada ao serviço antes de excluí-la manualmente.

> **Note**
>
> Se o serviço social AWS End User Messaging estiver usando a função ao mesmo tempo que você tenta 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 AWSServiceRoleForSocialMessaging

1. Ligue `list-linked-whatsapp-business-accounts` API para ver os recursos que você tem.
2. Para cada conta comercial vinculada do whats app, ligue `disassociate-whatsapp-business-account` API para o para remover o recurso do SocialMessaging serviço.
3. Verifique se nenhum recurso foi retornado ligando `list-linked-whatsapp-business-accounts` API novamente para o.

Como excluir manualmente a função vinculada ao serviço usando o IAM

Use o IAM console AWS CLI, o ou o AWS API para excluir a função AWSServiceRoleForSocialMessaging vinculada ao serviço. Para obter mais informações, consulte Excluindo uma função vinculada ao serviço no Guia do IAM usuário.

Regiões compatíveis com funções vinculadas AWS ao serviço do Application Auto Scaling

AWS O End User Messaging Social oferece suporte a funções vinculadas a serviços em todas as regiões nas quais o serviço esteja disponível. Para obter mais informações, consulte Regiões e endpoints da AWS.

Cotas para mensagens sociais para usuários AWS finais

A AWS conta da tem cotas padrão, anteriormente chamadas de limites, para cada AWS produto da. 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.

Para visualizar as cotas para AWS End User Messaging Social, abra o console do Service Quotas. No painel de navegação, escolha AWSserviços e selecione AWS End User Messaging Social.

Para solicitar o aumento da cota, consulte Solicitar um aumento de cota no Guia do usuário do Service Quotas. Se a cota ainda não estiver disponível no Service Quotas, use o formulário de aumento de limite.

A AWS conta da 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	Taxa
SendWhatsAppMessage	1.000
PostWhatsAppMessageMedia	100
GetWhatsAppMessageMedia	100
DeleteWhatsAppMessageMedia	100
DisassociateWhatsAppBusinessAccount	10
ListWhatsAppBusinessAccount	10
TagResource	10

Operation	Taxa
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 Main FleetWize.

Alteração	Descrição	Data
Lançamento inicial	Versão inicial do Guia do usuário do AWS End User Messaging Social	10 de julho 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.