Guide de l'utilisateur

AWS Messagerie sociale destinée aux utilisateurs finaux

AWS Messagerie sociale destinée aux utilisateurs finaux: Guide de l’utilisateur

Table of Contents

Qu'est-ce que la messagerie sociale destinée aux utilisateurs AWS finaux ?

AWS La messagerie sociale destinée aux utilisateurs finaux, également appelée messagerie sociale, est un service de messagerie qui permet aux développeurs de l' WhatsApp intégrer à leurs applications. Il donne accès aux riches fonctionnalités WhatsApp de messagerie de l'entreprise, permettant de créer du contenu interactif de marque avec des images, des vidéos et des boutons. En utilisant ce service, vous pouvez ajouter des fonctionnalités de WhatsApp messagerie à vos applications en plus des canaux existants tels que SMS les notifications push, ce qui vous permet d'interagir avec les clients via leur canal de communication préféré.

Pour commencer, vous pouvez soit créer un nouveau compte WhatsApp professionnel (WABA) à l'aide du processus d'intégration autoguidé dans la console sociale de messagerie de l'utilisateur AWS final, soit associer un compte existant WABA au service.

Rubriques

Vous utilisez Messaging Social pour AWS la première fois ?

Si vous utilisez AWS End User Messaging Social pour la première fois, nous vous recommandons de commencer par lire les sections suivantes :

- Configuration de la messagerie sociale pour les utilisateurs AWS finaux
- Commencer à utiliser AWS la messagerie sociale pour les utilisateurs finaux
- Bonnes pratiques en matière de messagerie sociale pour les utilisateurs AWS finaux

Caractéristiques de la messagerie sociale destinée aux utilisateurs AWS finaux

AWS L'utilisateur final Messaging Social fournit les fonctionnalités et capacités suivantes :

- Concevez des messages cohérents et réutilisez plus efficacement le contenu en créant et en utilisant des modèles de message. Un modèle de message contient du contenu et des paramètres que vous souhaitez réutiliser dans les messages que vous envoyez.
- Accédez à de nouvelles fonctionnalités de messagerie enrichies pour une expérience plus engageante. Au-delà du texte et des médias, vous pouvez envoyer des lieux et des messages interactifs.
- Recevez des SMS et des messages multimédia entrants de la part de vos clients.
- Renforcez la confiance de vos clients en vérifiant l'identité de votre entreprise via Meta.

Services connexes

AWS propose d'autres services de messagerie qui peuvent être utilisés conjointement dans un flux de travail multicanal :

- Utiliser AWS la messagerie de l'utilisateur final SMS pour envoyer SMS des messages
- Utiliser AWS la messagerie push à l'utilisateur final pour envoyer des notifications push
- Utiliser Amazon SES pour envoyer des e-mails

Accès à AWS la messagerie sociale destinée aux utilisateurs finaux

Vous pouvez accéder à AWS End User Messaging Social en utilisant les moyens suivants :

AWS Console sociale de messagerie pour utilisateurs finaux

Interface Web dans laquelle vous créez et gérez des ressources.

AWS Command Line Interface

Interagissez avec AWS des services à l'aide des commandes de votre shell de ligne de commande. La AWS Command Line Interface est prise en charge sur Windows, macOS et Linux. Pour plus d'informations à ce sujet AWS CLI, consultez le Guide de AWS Command Line

Interface l'utilisateur. Vous trouverez les AWS SMS commandes dans la référence des AWS CLI commandes.

AWS SDKs

Si vous êtes un développeur de logiciels qui préfère développer des applications utilisant des langages propres APIs au lieu d'envoyer une demande HTTP ou si vous fournissez des bibliothèquesHTTPS, AWS des exemples de code, des didacticiels et d'autres ressources. Ces bibliothèques offrent des fonctions de base qui automatisent les tâches, telles que la signature cryptographique des demandes, les nouvelles tentatives de demande et la gestion des réponses d'erreur. Ces fonctions vous aideront à démarrer plus efficacement. Pour de plus amples informations, veuillez consulter Outils pour créer sur AWS.

Disponibilité par région

AWS La messagerie sociale est disponible dans plusieurs pays en Amérique du Nord, Régions AWS en Europe, en Asie et en Océanie. Dans chaque région, AWS dispose de plusieurs zones de disponibilité. Ces zones de disponibilité sont physiquement isolées mais sont reliées par des connexions réseau privées, à latence faible, à débit élevé et à forte redondance. Ces zones de disponibilité sont utilisées pour fournir des niveaux très élevés de disponibilité et de redondance, tout en réduisant au minimum la latence.

Pour en savoir plus Régions AWS, consultez Spécifiez ce que Régions AWS votre compte peut utiliser dans le Référence générale d'Amazon Web Services. Pour obtenir la liste de toutes les régions dans lesquelles AWS End User Messaging Social est actuellement disponible et le point de terminaison de chaque région, voir Points de terminaison et quotas pour les points de AWS terminaison de AWS service API et de messagerie des utilisateurs finaux dans le tableau Référence générale d'Amazon Web Servicesou le tableau suivant. Pour plus d'informations sur le nombre de zones de disponibilité disponibles dans chaque région, consultez Infrastructure mondiale AWS.

Disponibilité dans les Régions

Nom de la région	Région	Point de terminaison	WhatsApp APIversion
US East (Virginie du Nord)	us-east-1	social-messaging.us-east-1.amazonaws.com	Version 20 et versions ultérieures

Nom de la région	Région	Point de terminaison	WhatsApp APIversion
		social-messaging-fips.us-east-1.api.aws social-messaging.us-east-1.api.aws	
USA Est (Ohio)	us-east-2	social-messaging.us-east-2.amazonaws.com social-messaging-fips.us-east-2.api.aws social-messaging.us-east-2.api.aws	Version 20 et versions ultérieures
USA Ouest (Oregon)	us-west-2	social-messaging.us-west-2.amazonaws.com social-messaging-fips.us-west-2.api.aws social-messaging.us-west-2.api.aws	Version 20 et versions ultérieures
Asie-Pacifique (Mumbai)	ap-south-1	social-messaging.ap-south-1.amazonaws.com social-messaging.ap-south-1.api.aws	Version 20 et versions ultérieures

Nom de la région	Région	Point de terminaison	WhatsApp APIversion
Asie-Pacifique (Singapour)	ap-southeast-1	social-messaging.ap-southeast-1.amazonaws.com social-messaging.ap-southeast-1.api.aws	Version 20 et versions ultérieures
Europe (Irlande)	eu-west-1	social-messaging.eu-west-1.amazonaws.com social-messaging.eu-west-1.api.aws	Version 20 et versions ultérieures
Europe (Londres)	eu-west-2	social-messaging.eu-west-2.amazonaws.com social-messaging.eu-west-1.api.aws	Version 20 et versions ultérieures

Configuration de la messagerie sociale pour les utilisateurs AWS finaux

Avant de pouvoir utiliser AWS End User Messaging Social pour la première fois, vous devez suivre la procédure ci-dessous.

Rubriques

S'inscrire à un Compte AWS

Si vous n'avez pas de compte Compte AWS, complétez les étapes suivantes pour en créer un.

Pour s'inscrire à un Compte AWS

1. Ouvrez l'https://portal.aws.amazon.com/billing/inscription.
2. Suivez les instructions en ligne.

   Dans le cadre de la procédure d'inscription, vous recevrez un appel téléphonique et vous saisirez un code de vérification en utilisant le clavier numérique du téléphone.

   Lorsque vous vous inscrivez à un Compte AWS, un Utilisateur racine d'un compte AWSest créé. Par défaut, seul l'utilisateur racine a accès à l'ensemble des Services AWS et des ressources de ce compte. La meilleure pratique de sécurité consiste à attribuer un accès administratif à un utilisateur, et à utiliser uniquement l'utilisateur racine pour effectuer les tâches nécessitant un accès utilisateur racine.

AWS vous envoie un e-mail de confirmation lorsque le processus d'inscription est terminé. Vous pouvez afficher l'activité en cours de votre compte et gérer votre compte à tout moment en accédant à https://aws.amazon.com/et en cliquant sur My Account (Mon compte).

Création d'un utilisateur doté d'un accès administratif

Une fois que vous vous êtes inscrit à un Compte AWS Utilisateur racine d'un compte AWS, sécurisez l' AWS IAM Identity Center, activez et créez un utilisateur administratif afin de ne pas utiliser l'utilisateur root pour les tâches quotidiennes.

Sécurisez votre Utilisateur racine d'un compte AWS

1. Connectez-vous à la en AWS Management Consoletant que propriétaire du compte en choisissant Root user (Utilisateur racine) et en saisissant l'adresse Compte AWS e-mail de. Sur la page suivante, saisissez votre mot de passe.

   Pour obtenir de l'aide pour vous connecter en utilisant l'utilisateur racine, consultez Connexion en tant qu'utilisateur racine dans le Guide de l'utilisateur Connexion à AWS .
2. Activez l'authentification multifactorielle (MFA) pour votre utilisateur root.

   Pour obtenir des instructions, voir Activer un MFA périphérique virtuel pour votre utilisateur Compte AWS root (console) dans le guide de IAM l'utilisateur.

Création d'un utilisateur doté d'un accès administratif

1. Activez IAM Identity Center.

   Pour obtenir des instructions, consultez Activation d' AWS IAM Identity Center dans le Guide de l'utilisateur AWS IAM Identity Center .
2. Dans IAM Identity Center, octroyez un accès administratif à un utilisateur.

   Pour un didacticiel sur l'utilisation du Répertoire IAM Identity Center comme source d'identité, voir Configurer l'accès utilisateur par défaut Répertoire IAM Identity Center dans le Guide de AWS IAM Identity Center l'utilisateur.

Connexion en tant qu'utilisateur doté d'un accès administratif

- Pour vous connecter avec votre utilisateur IAM Identity Center, utilisez l'identifiant URL qui a été envoyé à votre adresse e-mail lorsque vous avez créé l'utilisateur IAM Identity Center.

  Pour obtenir de l'aide afin de vous connecter à l'aide d'un utilisateur IAM Identity Center, consultez Connexion au portail AWS d'accès dans le Guide de Connexion à AWS l'utilisateur.

Attribution d'un accès à d'autres utilisateurs

1. Dans IAM Identity Center, créez un ensemble d'autorisations qui respecte la bonne pratique consistant à appliquer les autorisations de moindre privilège.

   Pour obtenir des instructions, consultez Création d’un ensemble d’autorisations dans le Guide de l’utilisateur AWS IAM Identity Center .
2. Attribuez des utilisateurs à un groupe, puis attribuez un accès par authentification unique au groupe.

   Pour obtenir des instructions, consultez Ajout de groupes dans le Guide de l’utilisateur AWS IAM Identity Center .

Étapes suivantes

Maintenant que vous êtes prêt à utiliser AWS End User Messaging Social, découvrez Commencer à utiliser AWS la messagerie sociale pour les utilisateurs finaux comment créer votre compte WhatsApp professionnel (WABA) ou migrer votre compte WhatsApp professionnel existant.

Commencer à utiliser AWS la messagerie sociale pour les utilisateurs finaux

Ces rubriques vous indiquent les étapes à suivre pour associer ou migrer votre compte WhatsApp professionnel (WABA) vers AWS Final User Messaging Social.

Rubriques

Inscription à WhatsApp

Un compte WhatsApp professionnel (WABA) permet à votre entreprise d'utiliser la plateforme WhatsApp commerciale pour envoyer des messages directement à vos clients. Vous faites tous partie de votre portefeuille d'activités Meta. WABAs A WABA contient les ressources destinées à vos clients, telles que le numéro de téléphone, les modèles et le profil WhatsApp professionnel. Un profil WhatsApp professionnel contient les coordonnées de votre entreprise que les utilisateurs peuvent consulter. Pour plus d'informations sur les comptes WhatsApp professionnels, consultezWhatsApp Compte professionnel (WABA) dans la messagerie sociale de l'utilisateur AWS final.

Suivez les étapes de cette section pour démarrer avec AWS End User Messaging Social. Utilisez le processus d'inscription intégré pour créer un nouveau compte WhatsApp professionnel (WABA) ou migrer un compte existant WABA vers AWS End User Messaging Social.

Prérequis

Important

Travailler avec Meta/ WhatsApp

- Votre utilisation de la solution WhatsApp professionnelle est soumise aux conditions générales des conditions d'utilisation WhatsApp commerciales, aux conditions de la solution WhatsApp commerciale, à la politique de messagerie WhatsApp professionnelle, aux directives de WhatsApp messagerie et à toutes les autres conditions, politiques ou directives qui y sont incorporées par référence (car chacune peut être mise à jour de temps à autre).

- Méta ou WhatsApp peut à tout moment vous interdire l'utilisation de la solution WhatsApp commerciale.
- Vous devez créer un compte WhatsApp professionnel (» WABA «) avec Meta et WhatsApp.
- Vous devez créer un compte Business Manager avec Meta et le lier à votreWABA.
- Vous devez nous en donner WABA le contrôle. À votre demande, nous vous transférerons le contrôle de votre WABA dos de manière raisonnable et rapide en utilisant les méthodes mises à notre disposition par Meta.
- Dans le cadre de votre utilisation de la solution WhatsApp commerciale, vous ne soumettrez aucun contenu, information ou donnée soumis à des mesures de sauvegarde et/ou à des limitations de distribution conformément aux lois et/ou réglementations applicables.
- WhatsApples tarifs d'utilisation de la solution WhatsApp professionnelle sont disponibles sur la page Tarification basée sur la conversation.

- Pour créer un compte WhatsApp professionnel (WABA), votre entreprise a besoin d'un compte Meta Business. Vérifiez si votre entreprise possède déjà un compte Meta Business. Si vous n'avez pas de compte Meta Business, vous pouvez en créer un au cours du processus d'inscription.
- Pour utiliser un numéro de téléphone déjà utilisé avec l'application WhatsApp Messenger ou l'application WhatsApp Business, vous devez d'abord le supprimer.
- Numéro de téléphone pouvant recevoir soit un code d'accès à usage unique SMS soit un code vocal à usage unique (OTP). Le numéro de téléphone utilisé pour l'inscription est associé à votre WhatsApp compte et le numéro de téléphone est utilisé lorsque vous envoyez des messages. Le numéro de téléphone peut toujours être utilisé pour SMSMMS, et pour la messagerie vocale.
- Si vous importez un numéro existantWABA, vous avez besoin PINs de tous les numéros de téléphone associés à l'importationWABA. Pour réinitialiser une solution perdue ou oubliéePIN, suivez les instructions de la section Mise PIN à jour du manuel WhatsApp Business Platform Cloud API Reference.

Inscrivez-vous via la console

Suivez ces instructions pour créer un nouveau WhatsApp compte, migrer votre compte existant ou ajouter un numéro de téléphone à un compte existantWABA. Dans le cadre du processus d'inscription, vous donnez à AWS Final User Messaging Social un accès à votre compte

WhatsApp professionnel. Vous autorisez également l'utilisateur AWS final Messaging Social à vous facturer les messages. Pour plus d'informations sur les comptes WhatsApp professionnels, consultezComprendre les types de comptes WhatsApp professionnels.

1. Ouvrez la console sociale de messagerie utilisateur AWS final à l'adresse https://console.aws.amazon.com/social-messaging/.
2. Choisissez Comptes professionnels.
3. Sur la page Associer un compte professionnel, sélectionnez Lancer le portail Facebook. Une nouvelle fenêtre de connexion de Meta apparaîtra.
4. Dans la fenêtre de méta-connexion, saisissez les informations d'identification de votre compte Facebook.

   Sur la page du compte WhatsApp professionnel, choisissez Ajouter un WhatsApp numéro de téléphone. Sur la page Ajouter un numéro de WhatsApp téléphone, choisissez Lancer le portail Facebook. Une nouvelle fenêtre de connexion de Meta apparaîtra.
5. Dans la fenêtre de méta-connexion, saisissez les informations d'identification de votre compte Facebook.
6. Dans le cadre du processus d'inscription, vous accordez à l'utilisateur AWS final un accès social à votre compte WhatsApp professionnel (WABA). Vous autorisez également l'utilisateur AWS final Messaging Social à vous facturer les messages. Choisissez Continuer.
7. Pour le compte Meta Business, choisissez un compte Meta business existant ou créez un compte Meta Business.

   a. (Facultatif) Si vous devez créer un compte Meta Business, procédez comme suit :

   b. Dans Nom de l'entreprise, entrez le nom de votre entreprise.

   c. Pour le site Web ou la page de profil de votre entreprise, saisissez le URL site Web de votre entreprise ou, si votre entreprise n'a pas de site Web, accédez URL à votre page de réseau social.

   d. Dans le champ Pays, choisissez le pays dans lequel se trouve votre entreprise.

   e. (Facultatif) Choisissez Ajouter une adresse et saisissez l'adresse de votre entreprise.
8. Choisissez Suivant.
9. Pour Choisir un compte WhatsApp professionnel, choisissez un compte WhatsApp professionnel existant (WABA), ou si vous devez créer un compte, choisissez Créer un compte WhatsApp professionnel.

Pour Créer ou sélectionner un profil WhatsApp professionnel, choisissez un profil WhatsApp professionnel existant ou créez un nouveau profil WhatsApp professionnel.

10. Choisissez Suivant.
11. Pour créer un profil professionnel, entrez les informations suivantes :

    - Dans le WhatsApp champ Nom du compte professionnel, entrez le nom de votre compte. Ce champ n'est pas destiné au client.
    - Pour le nom d'affichage du profil WhatsApp professionnel, entrez le nom à afficher à vos clients lorsqu'ils reçoivent un message de votre part. Nous vous recommandons d'utiliser le nom de votre entreprise comme nom d'affichage. Le nom est revu par Meta et doit être conforme aux règles relatives aux noms WhatsApp d'affichage. Pour utiliser un nom de marque différent du nom de votre entreprise, il doit exister une association publiée en externe entre votre entreprise et la marque. Cette association doit être affichée sur votre site Web et sur la marque représentée par le site Web du nom d'affichage.

      Une fois l'enregistrement terminé, Meta passe en revue votre nom d'affichage. Meta vous envoie un e-mail vous indiquant si le nom d'affichage a été approuvé ou rejeté. Si votre nom d'affichage est refusé, votre limite quotidienne de messagerie est abaissée et vous risquez d'être déconnecté de WhatsApp.

      > ⚠ Important
      >
      > Pour modifier votre nom d'affichage, vous devez créer un ticket avec le support Meta.

    - Pour Fuseau horaire, choisissez le fuseau horaire dans lequel se trouve l'entreprise.
    - Dans Catégorie, choisissez la catégorie qui correspond le mieux à votre activité. Les clients peuvent consulter votre catégorie dans le cadre de vos coordonnées.
    - Pour Description de l'entreprise, saisissez une description de votre entreprise. Les clients peuvent consulter la description de votre entreprise dans le cadre de vos coordonnées.
    - Dans Site Web, entrez le site Web de votre entreprise. Les clients peuvent consulter votre site Web dans le cadre de vos coordonnées.
    - Choisissez Suivant.
12. Pour Ajouter un numéro de téléphone pour WhatsApp, entrez un numéro de téléphone pour vous inscrire. Ce numéro de téléphone est affiché à vos clients lorsque vous leur envoyez un message.

13. Pour Choisissez la manière dont vous souhaitez vérifier votre numéro, choisissez Message texte ou Appel téléphonique.

    - Lorsque vous êtes prêt à recevoir le code de vérification, choisissez Next.
    - Entrez le code de vérification, puis choisissez Next.

14. Une fois que votre numéro a été vérifié, vous pouvez choisir Next pour fermer la fenêtre dans Meta.
15. Pour les comptes WhatsApp professionnels, développez les balises. Cette option est facultative pour ajouter des balises à votre compte WhatsApp professionnel.

    Les balises sont des paires de clés et de valeurs que vous pouvez éventuellement appliquer à vos AWS ressources pour contrôler l'accès ou l'utilisation. Choisissez Ajouter une nouvelle balise et entrez une paire clé-valeur à joindre.

16. Un compte WhatsApp professionnel peut avoir un seul message et une seule destination d'événement pour enregistrer les événements relatifs au compte WhatsApp professionnel et à toutes les ressources associées au compte WhatsApp professionnel. Pour activer la journalisation des événements sur AmazonSNS, y compris la journalisation de la réception d'un message client, vous devez activer la publication des messages et des événements. Pour de plus amples informations, veuillez consulter Destinations des messages et des événements dans AWS End User Messaging Social.

    > **Important**
    >
    > Pour pouvoir répondre aux messages des clients, vous devez activer la publication des messages et des événements.

    Dans la section Informations sur la destination des messages et des événements, activez la publication d'événements. Pour AmazonSNS, choisissez soit un nouveau sujet SNS standard Amazon et entrez un nom dans le champ Nom du sujet, soit choisissez un sujet SNS standard Amazon existant et choisissez un sujet dans la liste déroulante Rubrique arn.

17. Sous Numéros de téléphone :

    Pour chaque numéro de téléphone sous Numéros de WhtsApp téléphone :

a. Pour vérifier le numéro de téléphone, entrez le code existant PIN ou entrez un nouveau PIN code. Pour réinitialiser une solution perdue ou oubliéePIN, suivez les instructions de la section Mise PIN à jour du manuel WhatsApp Business Platform Cloud API Reference.

b. Pour un réglage supplémentaire :

   i. Pour la région de localisation des données (facultatif), choisissez l'une des régions de Meta dans laquelle vous souhaitez stocker vos données au repos. Pour plus d'informations sur les politiques de confidentialité des données de Meta, consultez les sections Confidentialité et sécurité des données et Stockage API local dans le cloud dans le WhatsApp Business Platform Cloud API Reference.

   ii. Les balises sont des paires de clés et de valeurs que vous pouvez éventuellement appliquer à vos AWS ressources pour contrôler l'accès ou l'utilisation. Choisissez Ajouter une nouvelle balise et entrez une paire clé-valeur à joindre.

18. Un compte WhatsApp professionnel peut avoir un seul message et une seule destination d'événement pour enregistrer les événements relatifs au compte WhatsApp professionnel et à toutes les ressources associées au compte WhatsApp professionnel. Pour activer la journalisation des événements sur AmazonSNS, y compris la journalisation de la réception d'un message client, vous devez activer la publication des messages et des événements. Pour de plus amples informations, veuillez consulter Destinations des messages et des événements dans AWS End User Messaging Social.

> **Important**
>
> Vous devez activer la publication des messages et des événements pour pouvoir répondre aux messages des clients.

Dans la section Informations sur la destination des messages et des événements, activez la publication d'événements. Pour AmazonSNS, choisissez soit un nouveau sujet SNS standard Amazon et entrez un nom dans le champ Nom du sujet, soit choisissez un sujet SNS standard Amazon existant et choisissez un sujet dans la liste déroulante Rubrique arn.

19. Pour terminer la configuration, choisissez Ajouter un numéro de téléphone.

Étapes suivantes

Une fois que vous avez terminé l'inscription, vous pouvez commencer à envoyer des messages. Lorsque vous êtes prêt à commencer à envoyer des messages à grande échelle, effectuez la vérification commerciale. Maintenant que votre compte WhatsApp professionnel et vos comptes sociaux de messagerie pour utilisateurs AWS finaux sont liés, consultez les rubriques suivantes :

- Découvrez la destination des événements pour enregistrer les événements et recevoir les messages entrants.
- Découvrez comment créer des modèles de messages.
- Découvrez comment envoyer un texto ou un message multimédia.
- Découvrez comment recevoir un message.
- Découvrez les comptes professionnels officiels pour avoir une coche verte à côté de votre nom d'affichage et augmenter le débit de vos messages.

WhatsApp Compte professionnel (WABA) dans la messagerie sociale de l'utilisateur AWS final

Un compte WhatsApp professionnel (WABA) permet à votre entreprise d'utiliser la plateforme WhatsApp commerciale pour envoyer des messages directement à vos clients. Vous faites tous partie de votre portefeuille de méta-entreprises. WABAs Un compte WhatsApp professionnel contient des actifs destinés à vos clients, tels que le numéro de téléphone, les modèles et les coordonnées professionnelles. Un ne WABA peut exister que dans une seule Région AWS. Pour plus d'informations sur les comptes WhatsApp professionnels, consultez la section Comptes WhatsApp professionnels dans le guide WhatsApp Business Platform Cloud API Reference.

Important

Travailler avec Meta/ WhatsApp

- Votre utilisation de la solution WhatsApp professionnelle est soumise aux conditions générales des conditions d'utilisation WhatsApp commerciales, aux conditions de la solution WhatsApp commerciale, à la politique de messagerie WhatsApp professionnelle, aux directives de WhatsApp messagerie et à toutes les autres conditions, politiques ou directives qui y sont incorporées par référence (car chacune peut être mise à jour de temps à autre).
- Méta ou WhatsApp peut à tout moment vous interdire l'utilisation de la solution WhatsApp commerciale.
- Vous devez créer un compte WhatsApp professionnel (» WABA «) avec Meta et WhatsApp.
- Vous devez créer un compte Business Manager avec Meta et le lier à votreWABA.
- Vous devez nous en donner WABA le contrôle. À votre demande, nous vous transférerons le contrôle de votre WABA dos de manière raisonnable et rapide en utilisant les méthodes mises à notre disposition par Meta.
- Dans le cadre de votre utilisation de la solution WhatsApp commerciale, vous ne soumettrez aucun contenu, information ou donnée soumis à des mesures de sauvegarde et/ou à des limitations de distribution conformément aux lois et/ou réglementations applicables.

- WhatsAppLes tarifs d'utilisation de la solution WhatsApp professionnelle sont disponibles sur https://developers.facebook.com/docs/whatsapp/pricing.

Rubriques

Afficher un compte WhatsApp professionnel (WABA) dans AWS Final User Messaging Social

Suivez ces instructions pour voir ce qui vous est WABA associé Compte AWS.

1. Ouvrez la console sociale de messagerie utilisateur AWS final à l'adresse https://console.aws.amazon.com/social-messaging/.
2. Dans Comptes professionnels, choisissez unWABA.
3. Dans l'onglet Numéros de téléphone, affichez votre numéro de téléphone, votre nom d'affichage, votre niveau de qualité et le nombre de conversations professionnelles qu'il vous reste pour la journée.

   Dans l'onglet Destinations d'événements, consultez la destination de votre événement. Pour modifier la destination de votre événement, suivez les instructions indiquées dansDestinations des messages et des événements dans AWS End User Messaging Social.

   Dans l'onglet Modèles, choisissez Gérer les modèles de messages pour modifier vos WhatsApp modèles via Meta. WABAChacun d'entre eux est limité à 250 modèles.

   Dans l'onglet Tags, vous pouvez gérer vos balises de WABA ressources.

Ajouter un compte WhatsApp professionnel (WABA) dans AWS Final User Messaging Social

Ajoutez-en un nouveau WABA à votre compte si vous avez déjà un profil WhatsApp professionnel. Dans le cadre de la création d'un nouveau, WABA vous devez ajouter un numéro de téléphone auWABA.

- Pour ajouter un nouveau compte WABA à votre compte, suivez les étapes ci-dessous Commencer à utiliser AWS la messagerie sociale pour les utilisateurs finaux :
  - À l'étape 8, choisissez votre profil WhatsApp professionnel et choisissez Créer un nouveau compte WhatsApp professionnel.

Comprendre les types de comptes WhatsApp professionnels

Votre compte WhatsApp professionnel détermine la façon dont vous apparaissez aux yeux de vos clients. Lorsque vous créez un WhatsApp compte, celui-ci devient un compte professionnel. WhatsApp comprend deux types de comptes décisionnelle :

- Compte professionnel : WhatsApp vérifie l'authenticité de chaque compte sur la plateforme WhatsApp professionnelle. Si un compte professionnel a terminé le processus de vérification d'entreprise, le nom de l'entreprise sera visible par les utilisateurs même s'ils n'ont pas ajouté l'entreprise à leur carnet d'adresses. Cette fonctionnalité aide les utilisateurs à identifier les comptes professionnels vérifiés sur WhatsApp.
- Compte professionnel officiel : Outre les avantages d'un compte professionnel, un compte professionnel officiel possède un badge vert à cocher dans son profil et dans les en-têtes des fils de discussion.

  L'approbation d'un compte professionnel WhatsApp officiel (OBA) nécessite de fournir la preuve que l'entreprise est connue et reconnue par les consommateurs, par exemple par le biais d'articles, de billets de blog ou de critiques indépendantes. L'approbation d'un n' WhatsApp OBAest pas garantie, même si l'entreprise fournit la documentation requise. Le processus d'approbation est soumis à l'examen et à l'approbation de WhatsApp. WhatsApp ne divulgue pas publiquement les critères spécifiques qu'elle utilise pour évaluer et approuver les demandes de comptes professionnels officiels. Les entreprises qui le souhaitent WhatsApp OBA doivent démontrer leur réputation et leur reconnaissance, mais l'approbation finale est à la discrétion de WhatsApp.

Lorsque vous créez un WhatsApp compte, celui-ci devient un compte professionnel. Vous pouvez fournir à vos clients des informations sur votre entreprise, telles que le site Web, l'adresse et les heures d'ouverture. Pour les entreprises qui n'ont pas terminé la validation WhatsApp commerciale, le nom d'affichage apparaît uniquement en petit texte à côté du numéro de téléphone dans la vue des contacts, et non dans la liste des discussions ou dans le chat individuel. Une fois la vérification Meta Business terminée, le nom d'affichage de WhatsApp l'expéditeur sera affiché dans la liste de discussion et dans les fils de discussion individuels.

Ressources supplémentaires

- Pour plus d'informations sur le compte professionnel et le compte professionnel officiel, consultez la section Comptes professionnels dans le guide WhatsApp Business Platform Cloud API Reference.
- Pour plus d'informations sur le processus de vérification commerciale, consultez la section Vérification commerciale dans le manuel WhatsApp Business Platform Cloud API Reference.

Numéros de téléphone dans AWS Final User Messaging Social

Tous les comptes WhatsApp professionnels contiennent un ou plusieurs numéros de téléphone utilisés pour vérifier votre identité WhatsApp et sont utilisés dans le cadre de votre identité d'expéditeur. Vous pouvez associer plusieurs numéros de téléphone à un compte WhatsApp professionnel (WABA) et utiliser chaque numéro de téléphone pour une marque différente.

Rubriques

Considérations relatives au numéro de téléphone à utiliser avec un compte WhatsApp professionnel

Lorsque vous associez un numéro de téléphone à votre compte WhatsApp professionnel (WABA), vous devez tenir compte des points suivants :

- Les numéros de téléphone ne peuvent être associés qu'à un seul numéro WABA à la fois.
- Le numéro de téléphone peut toujours être utilisé pour SMSMMS, et les appels vocaux.
- Chaque numéro de téléphone bénéficie d'une note de qualité attribuée par Meta.

Vous pouvez obtenir un numéro de téléphone SMS compatible par le biais de la messagerie à l'utilisateur AWS final SMS en procédant comme suit :

1. Assurez-vous que le pays ou la région du numéro de téléphone est compatible avec le mode bidirectionnelSMS.

2. Demandez le numéro de téléphone. Selon le pays ou la région, il peut vous être demandé d'enregistrer le numéro de téléphone.
3. Activez la SMS messagerie bidirectionnelle pour le numéro de téléphone. Une fois la configuration terminée, vos SMS messages entrants sont envoyés vers une destination d'événement.

Ajouter un numéro de téléphone à un compte WhatsApp professionnel (WABA)

Vous pouvez ajouter des numéros de téléphone à un compte WhatsApp professionnel existant (WABA) ou créer un nouveau WABA numéro de téléphone.

Prérequis

Avant de commencer, les conditions suivantes doivent être remplies :

- Le numéro de téléphone doit pouvoir recevoir soit un code d'accès à usage unique SMS soit un code vocal à usage unique (OTP). Il s'agit du numéro de téléphone qui est ajouté à votreWABA.
- Le numéro de téléphone ne doit pas être associé à un autreWABA.

Ajouter un numéro de téléphone à un WABA

Pour ajouter un nouveau numéro de téléphone à votre numéro de téléphone existant WABA

1. Ouvrez la console sociale de messagerie utilisateur AWS final à l'adresse https://console.aws.amazon.com/social-messaging/.
2. Choisissez Comptes professionnels, puis Ajouter un WhatsApp numéro de téléphone.
3. Sur la page Ajouter un numéro de WhatsApp téléphone, choisissez Lancer le portail Facebook. Une nouvelle fenêtre de connexion de Meta apparaîtra.
4. Dans la fenêtre de connexion Meta, entrez les informations d'identification de votre compte de développeur Meta et choisissez votre portefeuille d'entreprises.
5. Choisissez le profil WABA et le profil WhatsApp professionnel auxquels vous voulez ajouter de numéro de téléphone.
6. Choisissez Suivant.

7. Pour Ajouter un numéro de téléphone pour WhatsApp, entrez un numéro de téléphone pour vous inscrire. Ce numéro de téléphone est affiché à vos clients lorsque vous leur envoyez un message.
8. Pour Choisissez la manière dont vous souhaitez vérifier votre numéro, choisissez Message texte ou Appel téléphonique.
9. Une fois que vous êtes prêt à recevoir le code de vérification, choisissez Next
10. Entrez le code de vérification, puis choisissez Next. Une fois que votre numéro a été vérifié, vous pouvez choisir Next pour fermer la fenêtre dans Meta.
11. Sous Numéros de WhtsApp téléphone :

    a. Pour vérifier le numéro de téléphone, entrez le code existant PIN ou entrez un nouveau PIN code. Pour réinitialiser une solution perdue ou oubliéePIN, suivez les instructions de la section Mise PIN à jour du manuel WhatsApp Business Platform Cloud API Reference.

    b. Pour un réglage supplémentaire :

        i. Pour Région de localisation des données (facultatif), choisissez l'une des régions de Meta dans laquelle vous souhaitez stocker vos données au repos. Pour plus d'informations sur les politiques de confidentialité des données de Meta, consultez les sections Confidentialité et sécurité des données et Stockage API local dans le cloud dans le WhatsAppBusiness Platform Cloud API Reference.

        ii. Les balises sont des paires de clés et de valeurs que vous pouvez éventuellement appliquer à vos AWS ressources pour contrôler l'accès ou l'utilisation. Choisissez Ajouter une nouvelle balise et entrez une paire clé-valeur à joindre.
12. Un compte WhatsApp professionnel peut avoir un seul message et une seule destination d'événement pour enregistrer les événements relatifs au compte WhatsApp professionnel et à toutes les ressources associées au compte WhatsApp professionnel. Pour activer la journalisation des événements sur AmazonSNS, y compris la journalisation de la réception d'un message client, activez la publication de messages et d'événements. Pour de plus amples informations, veuillez consulter Destinations des messages et des événements dans AWS End User Messaging Social.

> **⚠ Important**
>
> Vous devez activer la publication des messages et des événements pour pouvoir répondre aux messages des clients.

Dans la section Informations sur la destination des messages et des événements, activez la publication d'événements. Pour AmazonSNS, choisissez Nouveau sujet SNS standard Amazon et entrez un nom dans le champ Nom du sujet, ou choisissez Sujet SNS standard Amazon existant et choisissez un sujet dans la liste déroulante Rubrique arn.

13. Pour terminer la configuration, choisissez Ajouter un numéro de téléphone.

Afficher le statut d'un numéro de téléphone

Pour pouvoir envoyer des messages dans AWS End User Messaging Social, le statut du numéro de téléphone doit être Actif.

1. Ouvrez la console sociale de messagerie utilisateur AWS final à l'adresse https://console.aws.amazon.com/social-messaging/.
2. Choisissez les Numéros de téléphone.
3. Dans la section Numéros de téléphone, la colonne État indique le statut de chaque numéro de téléphone.

> **Note**
>
> Si le statut d'un numéro de téléphone est Configuration incomplète, vous pouvez choisir le numéro de téléphone, puis choisir Compléter la configuration pour terminer la configuration du numéro de téléphone.

Afficher l'identifiant d'un numéro de téléphone dans AWS Final User Messaging Social

Pour pouvoir envoyer des messages avec le AWS CLI, vous avez besoin de l'identifiant du numéro de téléphone pour identifier le numéro de téléphone à utiliser lors de l'envoi.

1. Ouvrez la console sociale de messagerie utilisateur AWS final à l'adresse https://console.aws.amazon.com/social-messaging/.
2. Choisissez les Numéros de téléphone.
3. Dans la section Numéros de téléphone, choisissez un numéro de téléphone.

4. La section Détails du numéro de téléphone contient l'identifiant du numéro de téléphone.

Augmentez les limites de conversation par messagerie dans WhatsApp

Les limites de messagerie font référence au nombre maximum de conversations qu'un numéro de téléphone professionnel peut ouvrir sur une période de 24 heures. Les numéros de téléphone professionnels sont initialement limités à 250 conversations initiées par une entreprise au cours d'une période de déménagement de 24 heures. Cette limite peut être augmentée par Meta en fonction de l'évaluation de la qualité de vos messages et du nombre de messages que vous envoyez. Les conversations initiées par l'entreprise ne peuvent utiliser que des modèles de messages.

Lorsqu'un client vous envoie un message, cela ouvre une fenêtre de service 24 heures sur 24. Pendant cette période, vous pouvez envoyer tous les types de messages.

Vous pouvez augmenter vous-même votre limite de messagerie à 1 000 messages en suivant les instructions suivantes :

- Votre numéro de téléphone professionnel doit avoir le statut Actif.
- Si la qualité de votre numéro de téléphone professionnel est faible, il peut continuer à être limité à 250 conversations initiées par une entreprise par jour jusqu'à ce que son niveau de qualité s'améliore.
- Faites une demande de vérification commerciale. Si votre entreprise est approuvée, la qualité de la messagerie sera analysée afin de déterminer si votre activité de messagerie justifie une augmentation de votre limite de messagerie. Sur la base de l'analyse, votre demande d'augmentation de la limite de messagerie sera approuvée ou refusée par Meta.
- Faites une demande de vérification d'identité. Si vous terminez la vérification d'identité et que votre identité est confirmée, Meta approuvera une augmentation de la limite de messagerie.
- Ouvrez au moins 1 000 conversations initiées par l'entreprise sur une période de déménagement de 30 jours à l'aide d'un modèle bénéficiant d'une note de qualité élevée. Une fois que vous aurez atteint le seuil de 1 000 conversations, la qualité de votre messagerie sera analysée afin de déterminer si votre activité de messagerie justifie une augmentation de votre limite de messagerie. L'objectif est d'envoyer régulièrement des messages de haute qualité afin d'augmenter potentiellement votre limite de messagerie.

Si vous avez effectué la vérification commerciale ou la vérification d'identité, ou si vous avez ouvert 1 000 conversations professionnelles ou plus, et que vous êtes toujours limité à 250 conversations initiées par une entreprise, envoyez une demande à Meta pour une mise à niveau du niveau des messages.

Si la vérification de votre entreprise ou de votre identité est rejetée, vous pouvez améliorer vos chances d'obtenir une approbation en envoyant des messages de haute qualité. En envoyant des messages de haute qualité, conformes et opt-in, l'activité et la qualité de vos messages peuvent être réévaluées, ce qui peut entraîner une augmentation de vos capacités de messagerie approuvées.

Le score de qualité de votre messagerie WhatsApp est calculé sur la base des commentaires et interactions récents des utilisateurs, une plus grande importance étant accordée aux données les plus récentes. Cela permet d'évaluer la qualité et la fiabilité globales de votre messagerie sur la plateforme.

Le niveau des limites de messages augmente

- 1 000 conversations initiées par des entreprises
- 10 000 conversations initiées par des entreprises
- 100 000 conversations initiées par des entreprises
- Un nombre illimité de conversations initiées par l'entreprise

Augmenter le débit des messages dans WhatsApp

Le débit de messages est le nombre de messages entrants et sortants par seconde (MPS) pour un numéro de téléphone. Par défaut, chaque numéro de téléphone possède un chiffre MPS de 80. Meta peut augmenter votre valeur MPS à 1 000 si vous respectez les conditions requises suivantes :

- Le numéro de téléphone doit pouvoir envoyer un nombre illimité de conversations initiées par l'entreprise
- Le numéro de téléphone doit avoir une note de qualité moyenne ou supérieure.

Comprendre l'évaluation de la qualité des numéros de téléphone dans WhatsApp

La qualité de votre numéro de téléphone et de vos messages est déterminée par Meta. Votre score de qualité de messagerie est basé sur la façon dont vos messages ont été reçus par les clients au

cours des 7 derniers jours, les messages les plus récents étant davantage pondérés. Le score de qualité de la messagerie est calculé sur la base d'une combinaison de signaux de qualité issus des conversations entre vous et vos WhatsApp utilisateurs. Ces signaux incluent les commentaires des utilisateurs tels que les blocages, les rapports et les raisons fournies par les utilisateurs lorsqu'ils bloquent une entreprise. Meta évalue la qualité de vos messages en fonction de la façon dont ils sont reçus par vos clients WhatsApp, en mettant l'accent sur les commentaires et interactions récents.

WhatsApp Évaluations de qualité des numéros de téléphone

- Vert : haute qualité
- Jaune : qualité moyenne
- Rouge : faible qualité

WhatsApp État des numéros de téléphone

- Connecté : vous pouvez envoyer des messages dans les limites de votre limite de messages.
- Signalé : La qualité de votre numéro de téléphone est faible et doit être améliorée. Si la qualité de votre téléphone ne s'améliore pas dans les 7 jours, le statut de votre numéro de téléphone passe à Connecté, mais la limite de conversations initiées par votre entreprise est abaissée d'un niveau.
- Restreint : vous avez atteint la limite de conversations initiées par votre entreprise pour la période de 24 heures en cours, mais vous pouvez toujours répondre aux messages clients entrants. Une fois le délai de 24 heures écoulé, vous pouvez à nouveau envoyer des messages.

Afficher l'évaluation de la qualité d'un numéro de téléphone

Suivez ces instructions pour voir la qualité d'un numéro de téléphone.

1. Ouvrez la console sociale de messagerie utilisateur AWS final à l'adresse https://console.aws.amazon.com/social-messaging/.
2. Dans Comptes professionnels, choisissez unWABA.
3. Dans l'onglet Numéros de téléphone, affichez votre numéro de téléphone, votre nom d'affichage, votre niveau de qualité et le nombre de conversations professionnelles qu'il vous reste pour la journée.

Utilisation de modèles de messages dans AWS End User Messaging Social

Vous pouvez utiliser des modèles de messages pour les types de messages que vous utilisez fréquemment, tels que les newsletters hebdomadaires ou les rappels de rendez-vous. Les modèles de messages sont le seul type de message qui peut être envoyé aux clients qui ne vous ont pas encore envoyé de message ou qui ne vous en ont pas envoyé au cours des dernières 24 heures.

Meta attribue à chaque modèle une note de qualité et un statut. L'évaluation de la qualité a un impact sur le statut d'un modèle et réduit le rythme ou le taux d'envoi du modèle.

Les modèles sont associés à votre compte WhatsApp professionnel (WABA), gérés par le biais du WhatsApp gestionnaire et révisés par WhatsApp.

Vous pouvez envoyer les types de modèles suivants :

- Basé sur du texte
- Basé sur les médias
- Message interactif
- Basée sur la localisation
- Modèles d'authentification avec boutons de mot de passe à usage unique
- Modèles de messages multi-produits

Meta fournit des modèles d'échantillons pré-approuvés. Pour en savoir plus, consultez la section Exemples de modèles de messages.

Pour plus d'informations sur les types de modèles de messages, consultez la section Modèle de message dans le WhatsApp Business Platform Cloud API Reference.

Utilisation de modèles de messages avec le WhatsApp gestionnaire

Utilisez le WhatsAppgestionnaire pour créer, modifier ou vérifier le statut d'un modèle.

1. Ouvrez la console sociale de messagerie utilisateur AWS final à l'adresse https://console.aws.amazon.com/social-messaging/.

2. Choisissez un compte professionnel, puis unWABA.
3. Dans l'onglet Modèles de messages, choisissez Gérer les modèles de messages. Le WhatsAppgestionnaire s'ouvre dans une nouvelle fenêtre dans laquelle vous pouvez gérer vos modèles en choisissant Modèles de messages.

Étapes suivantes

Une fois que vous avez créé ou modifié un modèle, vous devez le soumettre pour révision auprès de WhatsApp. L'évaluation de Meta peut prendre jusqu'à 24 heures. Meta envoie un e-mail à votre administrateur Business Manager et met à jour le statut du modèle dans le WhatsApp gestionnaire. Utilisez le WhatsAppgestionnaire pour vérifier le statut de votre modèle.

Comprendre le rythme des modèles WhatsApp

Le rythme des modèles est une méthode, utilisée par Meta, qui laisse le temps aux clients de faire part rapidement de leurs commentaires sur les modèles nouveaux ou modifiés. Il identifie et met en pause les modèles qui suscitent peu d'engagement ou de commentaires, ce qui vous laisse le temps d'ajuster le contenu du modèle avant de l'envoyer à un trop grand nombre de clients. Cela réduit le risque que les commentaires négatifs des clients aient un impact sur l'entreprise. Par exemple, si trop de clients « bloquent » votre message ou si le taux de lecture de votre modèle est faible, l'évaluation de la qualité de votre modèle peut être réduite.

Le rythme des modèles affecte les modèles nouvellement créés, les modèles qui n'ont pas été interrompus et les modèles dont la qualité n'est pas élevée. Le rythme des modèles est souvent déclenché par un historique de modèles de faible qualité ou en pause. Lorsqu'un modèle est rythmé, les messages utilisant ce modèle sont envoyés normalement jusqu'à un certain seuil déterminé par Meta. Ensuite, les messages suivants sont conservés pour laisser le temps aux clients de faire part de leurs commentaires. Si le feedback est positif, le rythme du modèle est ensuite augmenté. Si le feedback est négatif, le rythme du modèle est réduit, ce qui vous permet d'ajuster le contenu du modèle. Pour plus d'informations, voir Template pacing dans le WhatsApp Business Platform Cloud API Reference.

Obtenez des commentaires sur le statut réduit d'un modèle avec WhatsApp Manager

Meta fournit des informations sur la raison pour laquelle le statut d'un modèle a été abaissé. Utilisez les commentaires de Meta pour modifier le modèle et le soumettre pour réapprobation, utiliser un autre modèle ou modifier le comportement de votre application. Si vous modifiez le modèle de message et qu'il est réapprouvé, son niveau de qualité s'améliorera progressivement tant qu'il ne reçoit pas de commentaires négatifs fréquents ou de faibles taux de lecture.

1. Ouvrez la console sociale de messagerie utilisateur AWS final à l'adresse https://console.aws.amazon.com/social-messaging/.
2. Choisissez un compte professionnel, puis unWABA.
3. Dans l'onglet Modèles de messages, choisissez Gérer les modèles de messages. Le WhatsAppgestionnaire s'ouvre dans une nouvelle fenêtre.
4. Choisissez Modèles de message, puis survolez le modèle avec le pointeur de la souris. Une infobulle devrait apparaître avec des informations expliquant pourquoi la note a été abaissée.

Comprendre le statut et l'évaluation de la qualité d'un modèle dans WhatsApp

Une note de qualité est attribuée à chaque modèle de message en fonction de l'utilisation, des commentaires et de l'engagement des clients. Un modèle ne peut être utilisé que si le statut est Actif, mais la qualité détermine le rythme du modèle. Si un modèle de message reçoit régulièrement des commentaires négatifs ou présente un faible taux d'engagement, cela entraînera une modification du statut du modèle.

Meta modifie automatiquement le statut ou l'évaluation de qualité d'un modèle en fonction des commentaires et de l'engagement négatifs ou positifs. Si le statut de votre modèle change, vous recevrez une notification WhatsApp du responsable, un e-mail et une notification d'événement. Utilisez le WhatsAppgestionnaire pour vérifier le statut de votre modèle.

Si votre modèle est rejeté par WhatsApp, vous pouvez le modifier et le soumettre à nouveau pour approbation ou déposer un recours auprès WhatsApp de. Pour en savoir plus, consultez la section Appeals in the WhatsApp Business Platform Cloud API Reference.

État du modèle	Évaluation de la qualité	Signification
En révision		Le modèle de message est en cours de révision. Cette opération peut prendre jusqu'à 24 heures.
Refusée		Le modèle de message a été rejeté et vous pouvez faire appel.
Actif	En attente	Le modèle de message n'a pas reçu de commentaires sur la qualité ni d'informa tions sur le taux de lecture de la part des clients, mais il peut toujours être utilisé pour envoyer des messages.
Actif	Élevé	Le modèle de message n'a reçu que peu ou pas de commentaires négatifs des clients et peut être utilisé pour envoyer des messages.
Actif	Moyen	Le modèle de message a reçu des commentaires négatifs de la part des clients, ou des taux de lecture faibles, et peut être suspendu ou désactivé.
Actif	Faible	Le modèle de message a reçu des commentaires négatifs de la part des clients ou un faible taux de lecture. Les modèles de message présentant ce statut peuvent être utilisés, mais ils risquent

État du modèle	Évaluation de la qualité	Signification
		d'être suspendus ou désactivés. Lorsqu'un modèle passe au statut Active-Low, son envoi est suspendu. La première pause est de trois heures, la seconde de six heures, et la pause suivante désactive le modèle.
Paused		Le modèle de message a été suspendu en raison des commentaires négatifs récurrents des clients ou du faible taux de lecture.
Désactivées		Le modèle de message a été désactivé en raison des commentaires négatifs récurrents des clients.
Appel demandé		Un appel a été demandé.

Raisons pour lesquelles un modèle est rejeté dans WhatsApp

Si votre modèle de message est examiné et rejeté par Meta, vous recevrez un e-mail expliquant pourquoi le modèle a été rejeté. Vous pouvez contester le rejet ou modifier votre modèle de message. Voici quelques-unes des raisons courantes pour lesquelles Meta peut rejeter un modèle de message :

- Les paramètres des variables contiennent des caractères spéciaux, tels que #, $ ou %.
- Les paramètres variables sont absents, les bretelles bouclées ne correspondent pas ou ne sont pas séquentiels.

- Le modèle de message contient du contenu qui enfreint la politique WhatsApp commerciale ou la politique WhatsApps commerciale.

Pour plus d'informations, consultez la section Motifs de rejet courants dans le manuel WhatsApp Business Platform Cloud API Reference.

Destinations des messages et des événements dans AWS End User Messaging Social

Une destination d'événement est une SNS rubrique Amazon vers laquelle les WhatsApp événements sont envoyés. Lorsque vous activez la publication d'événements sur un SNS sujet Amazon, tous vos événements d'envoi et de réception sont envoyés vers le SNS sujet Amazon. Utilisez les événements pour surveiller, suivre et analyser le statut des messages sortants et des communications clients entrantes.

Chaque compte WhatsApp professionnel (WABA) peut avoir une destination pour un événement. Tous les événements provenant de toutes les ressources associées au compte WhatsApp professionnel sont enregistrés sur cette destination d'événement. Par exemple, vous pouvez avoir un compte WhatsApp professionnel associé à trois numéros de téléphone et tous les événements associés à ces numéros de téléphone sont enregistrés sur une seule destination.

Rubriques

Ajouter un message et une destination d'événement à AWS End User Messaging Social

Lorsque vous activez la publication de messages et d'événements, tous les événements générés par votre compte WhatsApp professionnel (WABA) sont envoyés au SNS sujet Amazon. Cela inclut les événements pour chaque numéro de téléphone associé à un compte WhatsApp professionnel. Un SNS sujet Amazon WABA peut y être associé.

Prérequis

Avant de commencer, les prérequis suivants doivent être respectés.

- (Facultatif) Pour utiliser un SNS sujet Amazon chiffré à l'aide de AWS KMS clés, vous devez accorder aux utilisateurs AWS finaux des autorisations sociales conformément à la politique de clés existante.

Ajouter un message et une destination d'événement

1. Ouvrez la console sociale de messagerie utilisateur AWS final à l'adresse https://console.aws.amazon.com/social-messaging/.
2. Choisissez un compte professionnel, puis choisissez unWABA.
3. Dans l'onglet Destination de l'événement, choisissez Modifier la destination.
4. Pour activer une destination d'événement, choisissez Activer.
5. Pour envoyer vos événements vers une nouvelle SNS destination Amazon, choisissez Nouveau sujet de SNS stand et entrez un nom dans Nom du sujet. Le SNS sujet Amazon est créé avec des autorisations permettant à l'utilisateur AWS final Messaging Social d'accéder au sujet.

   Pour envoyer vos événements vers une SNS destination Amazon existante, choisissez un sujet SNS standard existant, puis un sujet du formulaire Topic arn. Vous devez appliquer les autorisations suivantes au SNS sujet Amazon :

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

Règles relatives aux SNS rubriques Amazon cryptées

Vous pouvez utiliser SNS des rubriques Amazon chiffrées à l'aide de AWS KMS clés pour un niveau de sécurité supplémentaire. Cette sécurité accrue peut être utile si votre application gère des données privées ou sensibles. Pour plus d'informations sur le chiffrement des SNS rubriques Amazon à l'aide de AWS KMS clés, consultez Activer la compatibilité entre les sources d'événements des AWS services et les rubriques chiffrées dans le Guide pour développeur Amazon Simple Notification Service.

L'exemple d'instruction utilise les options, facultatif mais recommandé, `SourceAccount` et `SourceArn` pour éviter le problème de confusion des adjoints et seul le compte propriétaire de l'application AWS End User Messaging Social a accès à l'application. Pour plus d'informations sur le problème des adjoints confus, voir Le problème des adjoints confus dans le guide de IAM l'utilisateur.

La clé que vous utilisez doit être symétrique. Les SNS rubriques Amazon chiffrées ne prennent pas en charge les AWS KMS clés asymétriques.

La stratégie de clé doit être modifiée pour permettre à l'utilisateur AWS final de Messaging Social d'utiliser la clé. Suivez les instructions de la section Modification d'une politique clé, dans le guide du AWS Key Management Service développeur, pour ajouter les autorisations suivantes à la politique clé existante :

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

Étapes suivantes

Une fois que vous avez configuré votre SNS rubrique Amazon, vous devez abonner un point de terminaison à cette dernière. Le point de terminaison commencera à recevoir tous les messages publiés dans la rubrique associée. Pour plus d'informations sur l'abonnement à un sujet, consultez l'article S'abonner à un SNS sujet Amazon dans le manuel Amazon SNS Developer Guide.

Format des messages et des événements dans AWS End User Messaging Social

L'JSONobjet d'un événement contient l'en-tête et la WhatsApp JSON charge utile de l' AWS événement. Pour une liste de la charge utile et des valeurs des JSON WhatsApp notifications, voir Référence de charge utile des notifications Webhooks et état des messages dans le WhatsApp Business Platform Cloud Reference. API

AWS En-tête de l'événement social de messagerie à l'utilisateur final

L'JSONobjet d'un événement contient l'en-tête de l' AWS événement et WhatsApp JSON. L'en-tête contient les AWS identifiants ARNs de votre compte WhatsApp professionnel (WABA) et de votre numéro de téléphone.

```
{
  "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
}
```

Dans l'exemple d'événement précédent :

- *1234567890abcde* est l'WABAidentifiant de Meta.
- *abcde1234567890* est l'identifiant du numéro de téléphone de Meta.
- *fb2594b8a7974770b128a409e2example* est l'ID du compte WhatsApp professionnel (WABA).

- *976c72a700aac43eaf573ae050example* est l'identifiant du numéro de téléphone.

Exemple WhatsApp JSON de réception d'un SMS

Ce qui suit montre l'enregistrement d'un message texte entrant provenant de WhatsApp. Le JSON est généré par WhatsApp. Pour obtenir la liste des champs et leur signification, consultez la référence de charge utile des notifications des webhooks dans le document WhatsApp Business Platform Cloud API Reference.

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

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

Exemple WhatsApp JSON de réception d'un message multimédia

Ce qui suit montre l'enregistrement d'un événement pour un message multimédia entrant. Pour récupérer le fichier multimédia, utilisez la GetWhatsAppMessageMedia API commande. Pour une liste des champs et leur signification, voir Webhooks Notification Payload Reference

```
{
//AWS End User Messaging Social header
}
{
  "id": "365731266123456",
  "changes": [
    {
      "value": {
        "messaging_product": "whatsapp",
        "metadata": {
          "display_phone_number": "12065550100",
          "phone_number_id": "321010217760100"
        },
        "contacts": [
          {
            "profile": {
              "name": "Diego"
            },
            "wa_id": "12065550102"
          }
        ],
        "messages": [
          {
            "from": "14255550150",
            "id":
 "wamid.HBgLMTQyNTY5ODgzMDIVAgASGCBDNzBDRjM5MDU2ODEwMDkwREY4ODBDRDE0RjVGRkexample",
            "timestamp": "1723506230",
            "type": "image",
            "image": {
              "mime_type": "image/jpeg",
              "sha256": "BTD0xlqSZ7l02o+/upusiNStlEZhA/urkvKf143Uqjk=",
```

```
              "id": "530339869524171"
            }
          }
        ]
      },
      "field": "messages"
    }
  ]
}
```

WhatsApp statut des messages

Lorsque vous envoyez un message, vous recevez des mises à jour de statut concernant le message. Vous devez activer la journalisation des événements pour recevoir ces notifications, voirDestinations des messages et des événements dans AWS End User Messaging Social.

Statuts des messages

Le tableau suivant contient les statuts de message possibles.

Nom du statut	Description
deleted	Le client a supprimé le message, et vous devez également le supprimer s'il a été téléchargé sur votre serveur.
livré	Le message a été remis avec succès au client.
failed	Le message n'a pas pu être envoyé.
lire	Le client a lu le message. Ce statut n'est envoyé que si le client a activé la lecture des reçus.
envoyé	Le message a été envoyé mais est toujours en transit.
warning	Le message contient un article qui n'est pas disponible ou n'existe pas.

Ressources supplémentaires

Pour plus d'informations, consultez la section État des messages dans le manuel WhatsApp Business Platform Cloud API Reference.

Téléchargement de fichiers multimédia à envoyer avec WhatsApp

Lorsque vous envoyez ou recevez un fichier multimédia, il doit être stocké dans un compartiment Amazon S3. Le compartiment Amazon S3 doit se trouver dans le même Compte AWS emplacement Région AWS que votre compte WhatsApp professionnel (WABA). Ces instructions indiquent comment créer un compartiment Amazon S3, charger un fichier et le URL compiler dans le fichier. Pour plus d'informations sur les commandes Amazon S3, consultez Utiliser des commandes de haut niveau (s3) avec le AWS CLI. Pour plus d'informations sur la configuration du AWS CLI, consultez Configurer le AWS CLI dans le guide de AWS Command Line Interface l'utilisateur, Création d'un compartiment et Chargement d'objets dans le guide de l'utilisateur Amazon S3.

Vous pouvez également créer un fichier présigné URL pour le fichier multimédia. Avec un présignéURL, vous pouvez accorder un accès limité dans le temps aux objets et les télécharger sans qu'un tiers ait besoin d'informations d'identification ou d' AWS autorisations de sécurité.

Pour créer un compartiment Amazon S3, utilisez la commande create-compartiment AWS CLI . Sur la ligne de commande, entrez la commande suivante :

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

Dans la commande précédente :

- Remplacez *us-east-1* avec Région AWS ce dans WABA quoi vous vous trouvez.
- Remplacez *BucketName* par le nom du nouveau compartiment.

Pour copier un fichier dans le compartiment Amazon S3, utilisez la AWS CLI commande cp. Sur la ligne de commande, entrez la commande suivante :

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

Dans la commande précédente :

- Remplacez *SourceFilePathAndName* par le chemin du fichier et le nom du fichier à copier.
- Remplacez *BucketName* par le nom du compartiment.

- Remplacez *FileName* avec le nom à utiliser pour le fichier.

L'URL à utiliser lors de l'envoi est :

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

Pour créer un présigné URL, remplacez *user input placeholders* par vos propres informations.

```
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
```

Les articles retournés URL seront les suivants : `https://amzn-s3-demo-bucket1.s3.af-south-1.amazonaws.com/mydoc.txt?{Headers}`

Types et tailles de fichiers multimédia pris en charge dans WhatsApp

Lors de l'envoi ou de la réception d'un message multimédia, le type de fichier doit être pris en charge et sa taille doit être inférieure à la taille maximale. Pour plus d'informations, consultez la section Types de médias pris en charge dans le WhatsApp manuel Business Platform Cloud API Reference.

Types de fichiers multimédias

Formats audio

Type audio	Extension	MIMEType	Taille max.
AAC	.aac	audio/aac	16 Mo
AMR	.amr	audio/amr	16 Mo
MP3	.mp3	audio/mpeg	16 Mo
MP4L'audio	.m4a	audio/mp4	16 Mo
OGGL'audio	.ogg	audio/ogg	16 Mo

Formats de documents

Types de document	Extension	MIMEType	Taille max.
Texte	.texte	text/plain	100 Mo
Microsoft Excel	.xls, .xlsx	application/vnd.ms-excel, application/vnd.openxmlformats-officedocument.spreadsheetml.sheet	100 Mo
Microsoft Word	.doc, .docx	application/msword, application/vnd.openxmlformats-officedocument.wordprocessingml.document	100 Mo
Microsoft PowerPoint	.ppt, .pptx	application/vnd.ms-powerpoint, application/vnd.openxmlformats-officedocument.presentationml.presentation	100 Mo
PDF	.pdf	application/pdf	100 Mo

Formats d'image

Type d'image	Extension	MIMEType	Taille max.
JPEG	.jpeg	image/jpeg	5 Mo
PNG	.png	image/png	5 Mo

Formats d'autocollants

Type d'autocollant	Extension	MIMEType	Taille max.
Autocollant animé	.webp	image/webp	500 Ko
Autocollant statique	.webp	image/webp	100 Ko

Formats vidéo

Type de vidéo	Extension	MIMEType	Taille max.
3 GPP	.3 gp	vidéo/3gp	16 Mo
MP4Vidéo	.mp4	vidéo/mp4	16 Mo

WhatsApp types de messages

Cette rubrique répertorie les types de messages pris en charge et décrit leur utilisation. Pour obtenir la liste des types de messages, consultez la section Messages dans le WhatsApp Business Platform Cloud API Reference.

Type de message	Description
Texte	Envoyez un SMS ou URL à votre client
Multimédia	Envoyez un fichier audio, un document, une image, un autocollant ou un fichier vidéo. Vous pouvez également envoyer des liens vers le fichier multimédia.
Reaction	Envoyez un emoji en réaction à un message, comme un pouce levé
Modèle	Envoyer un modèle de message
Emplacement	Envoyer un emplacement
Contacts	Envoyer une carte de visite
Interactive	Envoyer un message interactif

Ressources supplémentaires

Pour obtenir la liste des objets de WhatsApp message, consultez la section Messages dans le WhatsApp Business Platform Cloud API Reference.

Envoi de messages via WhatsApp AWS Final User Messaging Social

Avant d'envoyer un message, vous devez avoir terminé de configurer votre WABA compte et votre utilisateur doit avoir accepté de recevoir des messages de votre part, voir. Obtenir une autorisation

Lorsqu'un utilisateur vous envoie un message, une minuterie de 24 heures appelée fenêtre de service client démarre ou s'actualise. Tous les types de messages, à l'exception des modèles de messages, ne peuvent être envoyés à un utilisateur que lorsqu'une fenêtre de service client est ouverte entre vous et l'utilisateur. Les modèles de messages peuvent être envoyés à un utilisateur à tout moment, à condition que celui-ci ait accepté de recevoir des messages de votre part.

Pour chaque message que vous envoyez ou recevez, un statut de message est généré et envoyé à la destination de l'événement. Si votre client ne s'est pas inscrit, WhatsApp un événement est généré avec un statut de message de`fail`. Vous devez activer un message et une destination d'événement pour recevoir le statut du message.

> **Important**
>
> Travailler avec Meta/ WhatsApp
>
> - Votre utilisation de la solution WhatsApp professionnelle est soumise aux conditions générales des conditions d'utilisation WhatsApp commerciales, aux conditions de la solution WhatsApp commerciale, à la politique de messagerie WhatsApp professionnelle, aux directives de WhatsApp messagerie et à toutes les autres conditions, politiques ou directives qui y sont incorporées par référence (car chacune peut être mise à jour de temps à autre).
> - Méta ou WhatsApp peut à tout moment vous interdire l'utilisation de la solution WhatsApp commerciale.
> - Dans le cadre de votre utilisation de la solution WhatsApp commerciale, vous ne soumettrez aucun contenu, information ou donnée soumis à des mesures de sauvegarde et/ou à des limitations de distribution conformément aux lois et/ou réglementations applicables.

Rubriques

- Exemple d'envoi d'un modèle de message dans AWS End User Messaging Social
- Exemple d'envoi d'un message multimédia dans AWS End User Messaging Social

Exemple d'envoi d'un modèle de message dans AWS End User Messaging Social

L'exemple suivant montre comment utiliser un modèle pour envoyer un message à votre client à l'aide du AWS CLI. Pour plus d'informations sur la configuration du AWS CLI, voir Configurer le AWS CLI dans le guide de AWS Command Line Interface l'utilisateur.

```
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
```

Dans la commande précédente, procédez comme suit :

- Remplacez *{PHONE_NUMBER}* par numéro de téléphone de vos clients.
- Remplacez *{ORIGINATION_PHONE_NUMBER_ID}* avec l'identifiant de votre numéro de téléphone.

Exemple d'envoi d'un message multimédia dans AWS End User Messaging Social

L'exemple suivant montre comment envoyer un message multimédia à votre client à l'aide du AWS CLI. Pour plus d'informations sur la configuration du AWS CLI, voir Configurer le AWS CLI dans le guide de AWS Command Line Interface l'utilisateur. Pour obtenir une liste des types de fichiers multimédia pris en charge, consultezTypes et tailles de fichiers multimédia pris en charge dans WhatsApp.

1. Chargez le fichier multimédia sur un compartiment Amazon S3, consultezTéléchargement de fichiers multimédia à envoyer avec WhatsApp.
2. Téléchargez le fichier multimédia à WhatsApp l'aide de la post-whatsapp-message-mediacommande. Une fois terminée avec succès, la commande renverra le *{MEDIA_ID}* qui est nécessaire pour envoyer le message multimédia.

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

Dans la commande précédente, procédez comme suit :

- Remplacez *{ORIGINATION_PHONE_NUMBER_ID}* avec l'identifiant de votre numéro de téléphone.
- Remplacez *{BUCKET}* par le nom du compartiment Amazon S3.
- Remplacez *{MEDIA_FILE}* par le nom du fichier multimédia.

Vous pouvez également télécharger à l'aide d'une URL présignée en utilisant à la `--source-s3-presigned-url` place de`--source-s3-file`. Vous devez ajouter des informations `Content-Type` dans le champ des en-têtes. Si vous utilisez les deux, un `InvalidParameterException` est renvoyé.

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

3. Utilisez la send-whatsapp-messagecommande pour envoyer le message multimédia.

```
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
```

Dans la commande précédente, procédez comme suit :

- Remplacez *{PHONE_NUMBER}* par numéro de téléphone de vos clients.
- Remplacez *{ORIGINATION_PHONE_NUMBER_ID}* avec l'identifiant de votre numéro de téléphone.
- Remplacez *{MEDIA_ID}* par l'ID multimédia renvoyé à l'étape précédente.

4. Lorsque vous n'avez plus besoin du fichier multimédia, vous pouvez le supprimer à WhatsApp l'aide de la delete-whatsapp-message-mediacommande. Cela supprime uniquement le fichier multimédia, WhatsApp et non votre compartiment Amazon S3.

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

Dans la commande précédente, procédez comme suit :

- Remplacez *{ORIGINATION_PHONE_NUMBER_ID}* avec l'identifiant de votre numéro de téléphone.
- Remplacez *{MEDIA_ID}* avec l'identifiant du média.

Répondre à un message reçu dans AWS End User Messaging Social

Avant de pouvoir recevoir un SMS ou un message multimédia, vous devez avoir terminé de configurer votre destination d'événement WABA et d'en configurer la destination. Lorsque vous recevez un message entrant, un événement est enregistré dans le SNS sujet Amazon de destination de l'événement. Vous devez vous abonner au point de terminaison Amazon SNS Topics pour recevoir une notification.

Pour un exemple d'événement lié à la réception d'un message multimédia, voirExemple WhatsApp JSON de réception d'un message multimédia. Pour plus d'informations sur la configuration du AWS CLI, voir Configurer le AWS CLI dans le guide de AWS Command Line Interface l'utilisateur. Pour accéder à la liste des types de fichiers multimédias pris en charge, consultezTypes et tailles de fichiers multimédia pris en charge dans WhatsApp.

> **Important**
>
> Pour recevoir un message entrant, vous devez avoir activé les destinations d'événements pour leWABA, voirAjouter un message et une destination d'événement à AWS End User Messaging Social.

Exemple de modification du statut d'un message pour qu'il soit lu avec AWS End User Messaging Social

Vous pouvez définir le statut du message de manière `read` à ce que l'utilisateur final affiche deux coches bleues sur son écran.

```
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
```

Dans la commande précédente, procédez comme suit :

- Remplacez *{ORIGINATION_PHONE_NUMBER_ID}* avec l'identifiant de votre numéro de téléphone.

- Remplacez *{MESSAGE_ID}* par l'identifiant unique du message. Utilisez la valeur du `id` champ dans l'objet du message du SNS sujet Amazon.

Exemple de réponse à un message avec réaction dans AWS End User Messaging Social

Vous pouvez ajouter une réaction au message, comme un pouce levé.

```
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
```

Dans la commande précédente, procédez comme suit :

- Remplacez *{PHONE_NUMBER}* par numéro de téléphone de vos clients.
- Remplacez *{MESSAGE_ID}* par l'identifiant unique du message. Utilisez la valeur du `id` champ dans l'objet du message du SNS sujet Amazon.
- Remplacez *{ORIGINATION_PHONE_NUMBER_ID}* avec l'identifiant de votre numéro de téléphone.

Télécharger un fichier multimédia depuis WhatsApp Amazon S3

Pour récupérer un fichier multimédia et l'enregistrer dans un compartiment Amazon S3, utilisez la get-whatsapp-message-mediacommande.

```
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
}
```

Dans la commande précédente, procédez comme suit :

- Remplacez *{BUCKET}* par le nom du compartiment Amazon S3.

- Remplacez *{MEDIA_ID}* avec la valeur du champ id de l'événement reçu. Pour un exemple d'événement multimédia entrant, voirExemple WhatsApp JSON de réception d'un message multimédia.
- Remplacez *{ORIGINATION_PHONE_NUMBER_ID}* avec l'identifiant de votre numéro de téléphone.

Pour récupérer le contenu multimédia du compartiment Amazon S3, utilisez la commande suivante :

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

Dans la commande précédente, procédez comme suit :

- Remplacez *{BUCKET}* par le nom du compartiment Amazon S3.
- Remplacez *{MEDIA_ID}* par le MEDIA _ID renvoyé à l'étape précédente.

Exemple de réponse à un message par une lecture et une réaction

Dans cet exemple, votre client, Diego, vous a envoyé un message disant « Bonjour » et vous lui répondez avec un accusé de réception et un emoji.

Prérequis

Vous devez avoir configuré un SNS sujet Amazon de destination pour l'événement et vous abonner à l'un des points de terminaison du sujet pour recevoir une notification indiquant que Diego a envoyé un message.

Répondant

1. Lorsque le message de Diego est reçu, un événement est publié sur les points de terminaison du sujet. Ce qui suit est un extrait de ce que le sujet publie.

   > **Note**
   >
   > Comme Diego a initié la conversation, cela ne compte pas dans les conversations initiées par votre entreprise.

   ```
   {
   ```

```
  "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. Pour montrer à Diego que vous avez reçu le message, réglez le statut sur`read`. Diego verra deux coches bleues à côté du message sur son appareil.

```
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
```

Dans la commande précédente, procédez comme suit :

- Remplacez *{ORIGINATION_PHONE_NUMBER_ID}* avec le numéro de téléphone auquel Diego a envoyé son message`phone-number-id-976c72a700aac43eaf573ae050example`.
- Remplacez *{MESSAGE_ID}* avec l'identifiant unique du message. Il s'agit de la même valeur que l'identifiant indiqué dans le message reçu`wamid.HBgLMTQyNTY5ODgzMDIVAgASGCBDNzBDRjM5MDU2ODEwMDkwREY4ODBDRDE0RjVGRk`

3. Tu peux envoyer une réaction de la main à Diego.

```
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
```

Dans la commande précédente, procédez comme suit :

- Remplacez *{PHONE_NUMBER}* avec le numéro de téléphone de Diego`14255550150`.
- Remplacez *{MESSAGE_ID}* avec l'identifiant unique du message. Il s'agit de la même valeur que l'identifiant indiqué dans le message reçu`wamid.HBgLMTQyNTY5ODgzMDIVAgASGCBDNzBDRjM5MDU2ODEwMDkwREY4ODBDRDE0RjVGRk`

- Remplacez *{ORIGINATION_PHONE_NUMBER_ID}* avec le numéro de téléphone auquel Diego a envoyé son message`phone-number-id-976c72a700aac43eaf573ae050example`.

Ressources supplémentaires

- Activez les destinations des événements pour enregistrer les événements et recevoir les messages entrants.
- Pour obtenir la liste des objets de WhatsApp message, consultez la section Messages dans le WhatsApp Business Platform Cloud API Reference.

Présentation des rapports d'utilisation et de WhatsApp facturation pour les utilisateurs AWS finaux Messaging Social

Le canal social de messagerie utilisateur AWS final génère un type d'utilisation qui contient cinq champs au format suivant :*Region code*-*MessagingType*-*ISO*-*FeeDescription*-*FeeType*. Il existe deux éléments de facturation possibles pour chaque WhatsApp conversation : le WhatsApp`ConversationFee`, et le AWS per`MessageFee`.

Lorsque vous lancez une conversation en envoyant un modèle de message, vous êtes facturé un WhatsApp `ConversationFee` et un AWS par. `MessageFee` Cela ouvre une fenêtre de 24 heures où chaque message que vous envoyez ou recevez du même client est facturé au comptant AWS . `MessageFee`

Le type de WhatsApp conversation et le détail de la tarification se trouvent sur la page Tarification basée sur la conversation dans le guide du développeur de la plateforme WhatsApp commerciale.

Le tableau suivant affiche les valeurs et les descriptions possibles pour les champs du type d'utilisation. Pour plus d'informations sur AWS la tarification des messages sociaux destinés aux utilisateurs finaux, consultez AWS la section Tarification des messages destinés aux utilisateurs finaux.

Champ	Options	Description
Region code	• USE1— Région USA Est (Virginie du Nord) • USE2— Région USA Est (Ohio) • USW1— Région USA Ouest (Oregon) • APS1— Région Asie-Pacifique (Mumbai) • APSE1— Région Asie-Pacifique (Singapour)	Le Région AWS préfixe qui indique d'où le WhatsApp message a été envoyé ou reçu.

Champ	Options	Description
	• EUW1— Région Europe (Irlande) • EUW2— Région Europe (Londres)	
MessagingType	`WhatsApp`	Ce champ indique le type de message envoyé.
ISO	Voir les pays pris en charge	Code de ISO pays à deux chiffres auquel le message a été envoyé.
FeeDescription	`ConversationFee` , `MessageFee`	Ce champ spécifie soit le, WhatsApp `ConversationFee` soit le AWS per`MessageFee` .

Champ	Options	Description
FeeType	`Authentication` , `Marketing` , `Service`, `Utility`, `Standard`	Ce champ affiche le type de conversation, le type de conversation utilisé ou indique le tarif standard par message. **`ConversationFee`** Catégories initiées par les entreprises • `Marketing` — Utilisé pour atteindre un large éventail d'objectifs, qu'il s'agisse de renforcer la notoriété, de stimuler les ventes ou de retargeter les clients. Les exemples incluent les annonces de nouveaux produits, services ou fonctionnalités, les promotions/offres ciblées et les rappels d'abandon de panier. • `Utility`— Utilisé pour suivre les actions ou les demandes des utilisateurs. Les exemples incluent la confirmation d'inscription, la gestion des commandes/des livraisons (par exemple, une mise à jour de livraison), les mises à jour du compte ou les alertes (par exemple un rappel de paiement) ou les enquêtes de feedback.

Champ	Options	Description
		• `Authentication` — Utilisé pour authentifier les utilisateurs à l'aide de codes d'accès à usage unique, potentiellement à plusieurs étapes du processus de connexion (par exemple, vérification du compte, récupération du compte et problèmes d'intégrité). • `Service`— Utilisé pour résoudre les demandes des clients. **`ConversationFee`** Catégories créées par l'utilisateur • `Service`— Utilisé pour résoudre les demandes des clients. Catégories de **`MessageFee`** • `Standard`— Frais par message envoyé ou reçu.

Lorsque vous lancez une conversation en envoyant un modèle de message, vous êtes facturé un `ConversationFee` par un`MessageFee`. Cela ouvre une fenêtre de 24 heures dans laquelle chaque modèle de message que vous envoyez au même client est facturé individuellement`MessageFee`. Pendant la fenêtre de 24 heures, les modèles de messages doivent être du même type, sinon une nouvelle conversation sera lancée.

Par exemple, si vous envoyez un modèle de message marketing à un client, vous êtes facturé pour le `ConversationFee` et`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
```

Si le client vous envoie un message et que vous répondez, l'ouverture d'une nouvelle `Service` conversation et d'un nouveau message vous est facturée.

```
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
```

Exemple 1 : envoi d'un modèle de message marketing

Par exemple, si vous envoyez un modèle de message marketing à un client, vous êtes facturé un WhatsApp `ConversationFee` et un AWS par. `MessageFee`

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

Exemple 2 : ouverture d'une conversation de service

Des frais de conversation s'appliquent lorsqu'une entreprise répond au message entrant d'un utilisateur qui tombe en dehors de toute fenêtre de conversation active de 24 heures initiée par l'entreprise. Dans ce scénario, vous êtes facturé un WhatsApp `ConversationFee` et un AWS `MessageFee` pour chaque message entrant et sortant.

```
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 Messagerie à l'utilisateur final, ISO codes de facturation sociaux et cartographie des frais de WhatsApp conversation

Pays de la société

Code de ISO pays à deux chiffres	Nom du pays	WhatsApp région de facturation des conversations
AF	Afghanistan	Régions Asie-Pacifique
AX	Îles Malouines	Autre
AL	Albanie	Reste de l'Europe centrale et orientale
DZ	Algérie	Afrique
AS	Samoa américaines	Autre
AD	Andorre	Autre
AO	Angola	Afrique
AI	Anguilla	Autre
AQ	Antarctique	Autre
AG	Antigua et Barbuda	Autre
AR	Argentine	Argentine
AM	Arménie	Reste de l'Europe centrale et orientale
AW	Aruba	Autre
CLIMATISATION	Île normale d'Afrique	Autre
AU	Australie	Régions Asie-Pacifique
AT	Autriche	Reste de l'Europe de l'Ouest
AZ	Azerbaïdjan	Reste de l'Europe centrale et orientale

Code de ISO pays à deux chiffres	Nom du pays	WhatsApp région de facturation des conversations
BS	Bahamas	Autre
BH	Bahreïn	ME : Moyen-Orient
BD	Bangladesh	Régions Asie-Pacifique
BB	Barbade	Autre
BY	Biélorussie	Reste de l'Europe centrale et orientale
BE	Belgique	Reste de l'Europe de l'Ouest
BZ	Belize	Autre
BJ	Bénin	Afrique
BM	Bermudes	Autre
BT	Bhoutan	Autre
BO	Bolivie	Reste de l'Amérique latine
BQ	Bonaire	Autre
BA	Bosnie-Herzégovine	Autre
BW	Botswana	Afrique
BV	Île Bouvet	Autre
BR	Brésil	Brésil
E/S	Territoire Britannique de l'Océan Indien	Autre
VG	Îles Vierges Britanniques	Autre
BN	Brunéi Darussalam	Autre

Code de ISO pays à deux chiffres	Nom du pays	WhatsApp région de facturation des conversations
BG	Bulgarie	Reste de l'Europe centrale et orientale
BF	BurkinaFaso	Afrique
BI	Burundi	Afrique
KH	Cambodge	Régions Asie-Pacifique
CM	Cameroun	Afrique
CA	Canada	Amérique du Nord
CV	Cap-Vert	Autre
KY	Iles Caïmans	Autre
CF	République centrafricaine	Autre
TD	Tchad	Afrique
CL	Chili	Chili
CN	Chine	Régions Asie-Pacifique
CX	Île Christmas	Autre
CC	Îles Cocos (Keeling)	Autre
CO	Colombie	Colombie
KM	Comores	Autre
CG	Congo	Autre
CD	Congo	Afrique
CK	Iles Cook	Autre

Code de ISO pays à deux chiffres	Nom du pays	WhatsApp région de facturation des conversations
CR	Costa Rica	Reste de l'Amérique latine
CI	Côte d'Ivoire	Afrique
HR	Croatie	Reste de l'Europe centrale et orientale
CW	Curaçao	Autre
CY	Chypre	Autre
CZ	République tchèque	Reste de l'Europe centrale et orientale
DK	Danemark	Reste de l'Europe de l'Ouest
DJ	Djibouti	Autre
DM	Dominique	Autre
DO	République Dominicaine	Reste de l'Amérique latine
EC	Equateur	Reste de l'Amérique latine
EG	Egypte	Egypte
SV	El Salvador	Reste de l'Amérique latine
GQ	Guinée équatoriale	Autre
ER	Érythrée	Afrique
EE	Estonie	Autre
ET	Ethiopie	Afrique
FK	Îles Malouines	Autre
FO	Iles Féroé	Autre

Code de ISO pays à deux chiffres	Nom du pays	WhatsApp région de facturation des conversations
FJ	Fidji	Autre
FI	Finlande	Reste de l'Europe de l'Ouest
FR	France	France
GF	Guyane française	Autre
PF	Polynésie française	Autre
TF	Terres australes et antarctiques françaises	Autre
GA	Gabon	Afrique
GM	Gambie	Afrique
GE	Géorgie	Reste de l'Europe centrale et orientale
DE	Allemagne	Allemagne
GH	Ghana	Afrique
GI	Gibraltar	Autre
GR	Grèce	Reste de l'Europe centrale et orientale
GL	Groenland	Autre
GD	Grenade	Autre
GP	Guadeloupe	Autre
GU	Guam	Autre
GT	Guatemala	Reste de l'Amérique latine

Code de ISO pays à deux chiffres	Nom du pays	WhatsApp région de facturation des conversations
GG	Guernesey	Autre
GN	Guinée	Autre
GW	Guinée-Bissau	Afrique
GY	Guyane	Autre
HT	Haïti	Reste de l'Amérique latine
HM	Heard et McDonald les îles	Autre
HN	Honduras	Reste de l'Amérique latine
HK	Hong Kong	Régions Asie-Pacifique
HU	Hongrie	Reste de l'Europe centrale et orientale
IS	Islande	Autre
IN	Inde	Inde
IN	Heure normale d'Afrique	Heure normale d'Afrique
ID	Indonésie	Indonésie
ID	Interne Indonésie	Interne Indonésie
IQ	Irak	ME : Moyen-Orient
IE	Irlande	Reste de l'Europe de l'Ouest
IM	Île de Man	Autre
IL	Israël	Israël
IT	Italie	Italie

Code de ISO pays à deux chiffres	Nom du pays	WhatsApp région de facturation des conversations
JM	Jamaïque	Reste de l'Amérique latine
JP	Japon	Régions Asie-Pacifique
JE	Jersey	Autre
JO	Jordanie	ME : Moyen-Orient
KZ	Kazakhstan	Autre
KE	Kenya	Afrique
KI	Kiribati	Autre
XK	Kosovo	Autre
KW	Koweït	ME : Moyen-Orient
KG	Kirghizstan	Autre
LA	Lao PDR	Reste Asie-Pacifique
LV	Lettonie	Reste de l'Europe centrale et orientale
LB	Liban	ME : Moyen-Orient
LS	Lesotho	Afrique
LR	Liberia	Afrique
LY	Libye	Afrique
LI	Liechtenstein	Autre
LT	Lituanie	Reste de l'Europe centrale et orientale
LU	Luxembourg	Autre

Code de ISO pays à deux chiffres	Nom du pays	WhatsApp région de facturation des conversations
MO	Macao	Autre
MK	Macédoine	Reste de l'Europe centrale et orientale
MG	Madagascar	Afrique
MW	Malawi	Afrique
MY	Malaisie	Malaisie
MV	Maldives	Autre
ML	Mali	Afrique
MT	Malte	Autre
MH	Îles Marshall	Autre
MQ	Martinique	Autre
MR	Mauritanie	Afrique
MU	Maurice	Autre
YT	Mayotte	Autre
MX	Mexique	Mexique
FM	Micronésie	Autre
MD	Moldavie	Reste de l'Europe centrale et orientale
MC	Monaco	Autre
MN	Mongolie	Reste Asie-Pacifique
ME	Monténégro	Autre

Code de ISO pays à deux chiffres	Nom du pays	WhatsApp région de facturation des conversations
MS	Montserrat	Autre
MA	Maroc	Afrique
MZ	Mozambique	Afrique
MM	Birmanie	Autre
NA	Namibie	Afrique
NR	Nauru	Autre
NP	Népal	Reste Asie-Pacifique
NL	Pays-Bas	Pays-Bas
NC	Nouvelle-Calédonie	Autre
NZ	Nouvelle-Zélande	Reste Asie-Pacifique
NI	Nicaragua	Reste de l'Amérique latine
NE	Niger	Afrique
NG	Nigeria	Nigeria
NU	Niué	Autre
NF	Île Norfolk	Autre
MP	Îles Mariannes du Nord	Autre
NO	Norvège	Reste de l'Europe de l'Ouest
OM	Oman	ME : Moyen-Orient
PK	Pakistan	Pakistan
PW	Palaos	Autre

Code de ISO pays à deux chiffres	Nom du pays	WhatsApp région de facturation des conversations
PS	Territoires palestiniens	Autre
PA	Panama	Reste de l'Amérique latine
PG	Papouasie-Nouvelle-Guinée	Reste Asie-Pacifique
PY	Paraguay	Reste de l'Amérique latine
PE	Pérou	Pérou
PH	Philippines	Reste Asie-Pacifique
PN	Pitcairn	Autre
PL	Pologne	Reste de l'Europe centrale et orientale
PT	Portugal	Reste de l'Europe de l'Ouest
PR	Porto Rico	Reste de l'Amérique latine
QA	Qatar	ME : Moyen-Orient
RE	La Réunion	Autre
RO	Roumanie	Reste de l'Europe centrale et orientale
RU	Fédération de Russie	Russie
RW	Rwanda	Afrique
SH	Saint-Barthélemy	Autre
KN	Saint Kitts et Nevis	Autre
LC	Sainte-Lucie	Autre
PM	Saint-Pierre-et-Miquelon	Autre

Code de ISO pays à deux chiffres	Nom du pays	WhatsApp région de facturation des conversations
VC	Saint-Vincent-et-les Grenadines	Autre
BL	Saint-Barthélemy	Autre
MF	Saint-Barthélemy	Autre
WS	Samoa	Autre
SM	Saint-Marin	Autre
ST	Sao Tomé et Principe	Autre
SA	Arabie saoudite	Arabie saoudite
SN	Sénégal	Afrique
RS	Serbie	Reste de l'Europe centrale et orientale
SC	Seychelles	Autre
SL	Sierra Leone	Afrique
SG	Singapour	Reste Asie-Pacifique
SX	Sint Maarten	Autre
SK	Slovaquie	Reste de l'Europe centrale et orientale
SI	Slovénie	Reste de l'Europe centrale et orientale
SB	Iles Salomon	Autre
SO	Somalie	Afrique

Code de ISO pays à deux chiffres	Nom du pays	WhatsApp région de facturation des conversations
ZA	Afrique du Sud	Afrique du Sud
GS	Géorgie du Sud et îles Sandwich du Sud	Autre
KR	Corée du Sud	Autre
SS	Soudan du Sud	Afrique
ES	Espagne	Espagne
LK	Sri Lanka	Reste Asie-Pacifique
SR	Suriname	Autre
SJ	Îles Svalbard et Île Jan Mayen	Autre
SZ	Swaziland	Afrique
SE	Suède	Reste de l'Europe de l'Ouest
CH	Suisse	Reste de l'Europe de l'Ouest
TW	Taïwan	Reste Asie-Pacifique
TJ	Tadjikistan	Reste Asie-Pacifique
TZ	Tanzanie	Afrique
TH	Thaïlande	Reste Asie-Pacifique
TL	Timor-Leste	Autre
TG	Togo	Afrique
TK	Tokélaou	Autre
TO	Tonga	Autre

Code de ISO pays à deux chiffres	Nom du pays	WhatsApp région de facturation des conversations
TT	Trinidad et Tobago	Autre
TA	Trist et Cunha	Autre
TN	Tunisie	Afrique
TR	Turquie	Turquie
TM	Turkménistan	Reste Asie-Pacifique
TC	Iles Turks et Caicos	Autre
TV	Tuvalu	Autre
UG	Ouganda	Afrique
UA	Ukraine	Reste de l'Europe centrale et orientale
AE	Emirats arabes unis	Emirats arabes unis
Go	Royaume-Uni	Royaume-Uni
ETATS-UNIS	États-Unis	Amérique du Nord
UY	Uruguay	Reste de l'Amérique latine
UM	Îles mineures éloignées des États-Unis	Autre
UZ	Ouzbékistan	Reste Asie-Pacifique
VU	Vanuatu	Autre
VA	Pays de la société	Autre
VE	Venezuela	Reste de l'Amérique latine
VN	Vietnam	Reste Asie-Pacifique

Code de ISO pays à deux chiffres	Nom du pays	WhatsApp région de facturation des conversations
VI	Îles Malouines	Autre
WF	Îles Wallis et Futuna	Autre
EH	Sahara occidental	Autre
YE	Yémen	ME : Moyen-Orient
ZM	Zambie	Afrique
ZW	Zimbabwe	Autre

Surveillance de AWS la messagerie des utilisateurs finaux sur les réseaux sociaux

La surveillance constitue une part importante de la gestion de la fiabilité, de la disponibilité et des performances d' AWS End User Messaging Social et de vos autres AWS solutions. AWSfournit les outils de surveillance suivants pour contrôler les messages sociaux de l'utilisateur AWS final, signaler les problèmes et déclencher des actions automatiques, si nécessaire :

- Amazon CloudWatch contrôle vos AWS ressources et les applications que vous exécutez sur AWS en temps réel. Vous pouvez collecter et suivre les métriques, créer des tableaux de bord personnalisés, et définir des alarmes qui vous informent ou prennent des mesures lorsqu'une métrique spécifique atteint un seuil que vous spécifiez. Par exemple, vous pouvez connaître CPU l'utilisation d'Amazon EC2 pour une CloudWatch piste ou d'autres métriques et démarrer automatiquement de nouvelles instances lorsque cela est nécessaire. Pour de plus amples informations, veuillez consulter le Guide de CloudWatch l'utilisateur Amazon.
- Amazon CloudWatch Logs permet de contrôler, stocker et accéder à vos fichiers journaux à partir d'EC2instances Amazon CloudTrail, et d'autres sources. CloudWatch Les journaux peuvent surveiller les informations contenues dans les fichiers journaux et vous avertir lorsque certains seuils sont atteints. Vous pouvez également archiver vos données de journaux dans une solution de stockage hautement durable. Pour de plus amples informations, veuillez consulter le Guide de l'utilisateur Amazon CloudWatch Logs.
- AWS CloudTrailcapture API les appels et les événements associés créés par ou au nom de votre AWS compte et envoie les fichiers journaux à un compartiment Amazon S3 que vous spécifiez. Vous pouvez identifier les utilisateurs et les comptes qui ont appelé AWS, l'adresse IP source à partir de laquelle les appels ont été émis, ainsi que le moment où les appels ont eu lieu. Pour plus d'informations, consultez le AWS CloudTrail Guide de l'utilisateur .

Surveillance de AWS la messagerie des utilisateurs finaux sur les réseaux sociaux avec Amazon CloudWatch

Vous pouvez surveiller l'utilisation de la messagerie sociale de l'utilisateur AWS final CloudWatch, qui collecte les données brutes et les transforme en métriques lisibles et disponibles en temps quasi réel. Ces statistiques sont enregistrées pour une durée de 15 mois ; par conséquent, vous pouvez accéder aux informations historiques et acquérir un meilleur point de vue de la façon dont votre service ou

application web s'exécute. Vous pouvez également définir des alarmes qui surveillent certains seuils et envoient des notifications ou prennent des mesures lorsque ces seuils sont atteints. Pour de plus amples informations, veuillez consulter le Guide de CloudWatch l'utilisateur Amazon.

Dans le cas de la messagerie sociale destinée aux utilisateurs AWS finaux`WhatsAppMessageFeeCount`, vous souhaiterez peut-être surveiller `WhatsAppConversationFeeCount` et déclencher une alarme lorsqu'un seuil de dépenses est atteint.

Les tableaux suivants répertorient les métriques et les dimensions que AWS End User Messaging Social exporte vers l'espace de `AWS/SocialMessaging` noms.

Mesure	Unité	Description
WhatsAppConversationFeeCount	Nombre	Le montant des frais de WhatsApp conversation
WhatsAppMessageFeeCount	Nombre	Le montant des frais de WhatsApp message

Dimension	Description
MessageFeeType	Les types de frais valides sont le service, le marketing, les services publics et l'authentification
DestinationCountryCode	Le ISO code à deux lettres du pays
WhatsAppPhoneNumberArn	L'arnaque du numéro de téléphone.

Enregistrement de la messagerie de l'utilisateur AWS final, des API appels sociaux à l'aide AWS CloudTrail

AWS ORC est intégré à, un service qui enregistre les actions effectuées par un utilisateur AWS CloudTrail, un rôle ou un service qui enregistre les actions effectuées par un utilisateur, un rôle ou un service qui enregistre les actions effectuées par un utilisateur Service AWS. CloudTrail capture

tous les API appels pour AWS la messagerie sociale de l'utilisateur final sous forme d'événements. Les appels enregistrés contiennent les AWS appels depuis la section sans serveur de AWS la console API OpenSearch. À l'aide des informations collectées par CloudTrail CloudTrail, vous pouvez déterminer la demande qui a été envoyée à et, l'adresse IP à AWS partir de laquelle la demande a été effectuée, l'auteur de la demande, la date de la demande

Chaque événement ou entrée de journal contient des informations sur la personne ayant initié la demande. Les informations relatives à l'identité permettent de déterminer :

- Si la demande a été effectuée avec des informations d'identification d'utilisateur root ou d'utilisateur root.
- L'opération a été effectuée à l'aide de la demande, la demande a été effectuée IAM à l'aide de l'.
- Si la demande a été effectuée avec les informations d'identification de sécurité temporaires d'un rôle ou d'un utilisateur fédéré.
- Si la requête a été effectuée par un autre Service AWS.

CloudTrail est actif dans votre compte Compte AWS lorsque vous créez le compte et vous avez automatiquement accès à l'historique des CloudTrail événements. L'Historique des CloudTrail événements fournit un enregistrement consultable, interrogeable, téléchargeable et immuable des 90 derniers jours des 90 derniers jours des événements de gestion d'une. Région AWS Pour plus d'informations, consultez la section Utilisation de l'historique des CloudTrail événements dans le guide de AWS CloudTrail l'utilisateur. La consultation de l'Historique des événements ne génère aucuns CloudTrail frais.

Pour un registre permanent des événements de Compte AWS votre compte, créez un enregistrement permanent des CloudTrailévénements de votre compte.

CloudTrail sentiers

Un journal de suivi permet CloudTrail à CloudTrail de livrer des fichiers journaux dans un compartiment Amazon S3. Tous les journaux de suivi que vous créez à l' AWS Management Console aide de l'. Vous pouvez uniquement créer un journal de suivi multi-régions à l'aide de l'. AWS CLI La création d'un journal de suivi multi-régions est une Régions AWS bonne pratique. Vous ne pouvez créer un journal de suivi à région unique qu'à l'aide de Région AWS l'. Pour plus d'informations sur les sentiers, consultez les sections Création d'un sentier pour votre organisation Compte AWS et Création d'un sentier pour une organisation dans le guide de AWS CloudTrail l'utilisateur.

Vous pouvez diffuser une copie de vos événements de gestion en cours à votre compartiment Amazon S3 sans frais depuis CloudTrail en CloudTrail créant un suivi. Pour plus d'informations sur la CloudTrail tarification, consultez la section AWS CloudTrail Tarification. Pour obtenir des informations sur la tarification Amazon S3, consultez Tarification Amazon S3.

CloudTrail Les magasins de données d'événement CloudTrail Lake

CloudTrail Lake vous permet d'exécuter SQL des requêtes basées sur vos événements. CloudTrail CloudTrail Lake convertit les événements existants au format JSON basé sur des lignes JSON au ORC format Apache ORC. ORCORC est un format de stockage en colonnes qui est optimisé pour une récupération rapide des données. Les événements sont agrégés dans des magasins de données d'événement. Ceux-ci constituent des collections immuables d'événements basées sur des critères que vous sélectionnez en appliquant des sélecteurs d'événements avancés. Les sélecteurs que vous appliquez à un magasin de données d'événement contrôlent les événements qui persistent et que vous pouvez interroger. Pour plus d'informations sur CloudTrail Lake, consultez la section Travailler avec AWS CloudTrail Lake dans le guide de AWS CloudTrail l'utilisateur.

CloudTrail Les magasins de données d'événement Lake et les requêtes entraînent des frais. Lorsque vous créez un magasin de données d'événement, vous choisissez l'option de tarification que vous voulez utiliser pour le magasin de données d'événement. L'option de tarification détermine le coût d'ingestion et de stockage des événements, ainsi que les périodes de conservation par défaut et maximale pour le magasin de données d'événement. Pour plus d'informations sur la CloudTrail tarification, consultez la section AWS CloudTrail Tarification.

AWS Messagerie à l'utilisateur final Événements liés aux données sociales dans CloudTrail

Les événements de données fournissent des informations sur les opérations de ressources effectuées sur ou dans une ressource (par exemple, lecture ou écriture de données dans un objet Amazon S3). Ils sont également connus sous le nom opérations de plans de données. Les événements de données sont souvent des activités dont le volume est élevé. Par défaut, les journaux CloudTrail ne consignent pas les événements. L'historique des CloudTrail événements n'enregistre pas les événements liés aux données.

Des frais supplémentaires s'appliquent pour les événements de données. Pour plus d'informations sur la CloudTrail tarification, consultez la section AWS CloudTrail Tarification.

Vous pouvez enregistrer les événements de données pour les types de ressources sociales de messagerie utilisateur AWS final à l'aide de la CloudTrail console ou CloudTrail API des opérations. AWS CLI Pour plus d'informations sur la façon de consigner les événements liés aux données, consultez les sections Enregistrement des événements liés aux données avec le AWS Management Console et Enregistrement des événements liés aux données avec le AWS Command Line Interface dans le Guide de AWS CloudTrail l'utilisateur.

Le tableau suivant répertorie les types de ressources sociales de messagerie pour les utilisateurs AWS finaux pour lesquels vous pouvez enregistrer des événements de données. La colonne Type d'événement de données (console) indique la valeur à choisir dans la liste des types d'événements de données de la CloudTrail console. La colonne de valeur resources.type indique la **`resources.type`** valeur que vous devez spécifier lors de la configuration de sélecteurs d'événements avancés à l'aide du ou. AWS CLI CloudTrail APIs La CloudTrail colonne Données APIs enregistrées indique les API appels enregistrés CloudTrail pour le type de ressource.

Type d'événement de données (console)	valeur resources.type	Données APIs enregistrées sur CloudTrail
Numéro de téléphone de messagerie sociale	`AWS::SocialMessaging::PhoneNumberId`	• DeleteWhatsAppMessageMedia • GetWhatsAppMessageMedia • PostWhatsAppMessageMedia • SendWhatsAppMessage

Vous pouvez configurer des sélecteurs d'événements avancés pour filtrer les `eventName`, `readOnly`, et `resources.ARN` des champs pour enregistrer uniquement les événements importants pour vous. Pour plus d'informations sur ces autorisations, consultez. AdvancedFieldSelectordans la AWS CloudTrail APIréférence.

AWS Messagerie à l'utilisateur final Événements de gestion sociale dans CloudTrail

Les événements de gestion fournissent des informations sur les opérations de gestion exécutées sur les ressources de votre compte Compte AWS. Ils sont également connus sous le nom opérations de plan de contrôle. Par défaut, les CloudTrail journaux enregistrent les événements de gestion.

AWS End User Messaging Social enregistre toutes les opérations du plan de contrôle de AWS End User Messaging Social en tant qu'événements de gestion. Pour obtenir la liste des opérations du plan de contrôle social de AWS End User Messaging Social auxquelles AWS End User Messaging Social se connecte CloudTrail, consultez le manuel AWS End User Messaging Social API Reference.

AWS Messagerie à l'utilisateur final Exemples d'événements sociaux

Un événement représente une demande individuelle émise à partir d'une source quelconque et comprend des informations sur l'APIaction demandée, la date et l'heure de l'action, les paramètres de la demande, etc. CloudTrail Les fichiers journaux CloudTrail ne constituent pas une série ordonnée retraçant les API appels d'API publics.

L'exemple suivant montre une entrée CloudTrail de journal qui illustre l'opération.

```
{
        "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"
        }
    }
```

Pour plus d'informations sur le contenu des CloudTrail enregistrements, voir le contenu des CloudTrail enregistrements dans le Guide de AWS CloudTrail l'utilisateur.

Bonnes pratiques en matière de messagerie sociale pour les utilisateurs AWS finaux

Cette section décrit plusieurs bonnes pratiques qui peuvent vous aider à améliorer votre engagement client et éviter la suspension de votre compte. Cependant, notez que cette section ne contient pas de conseils juridiques. Consultez toujours un avocat pour obtenir des conseils juridiques.

Pour obtenir la liste la plus récente des WhatsApp meilleures pratiques, consultez la Politique de messagerie WhatsApp professionnelle.

Rubriques

Up-to-date profil de l'entreprise

Maintenez un profil up-to-date WhatsApp professionnel précis qui inclut les coordonnées du service client, telles qu'une adresse e-mail, une adresse de site Web ou un numéro de téléphone. Assurez-vous que les informations fournies sont véridiques et ne constituent pas une fausse représentation ou ne se font pas passer pour une autre entreprise.

Obtenir une autorisation

N'envoyez pas de messages aux destinataires qui n'ont pas demandé explicitement à recevoir les types spécifiques de messages que vous prévoyez d'envoyer. Lorsque vous avez encore besoin d'aide, vous pouvez utiliser les ressources suivantes :

- Le processus d'inscription doit clairement informer la personne qu'elle consent à recevoir des messages ou des appels de votre entreprise. WhatsApp Vous devez indiquer explicitement le nom de votre entreprise.

- Vous êtes seul responsable de déterminer la méthode d'obtention du consentement facultatif. Assurez-vous que le processus d'inscription est conforme à toutes les lois applicables régissant vos communications. Fournissez tous les avis requis et obtenez toutes les autorisations nécessaires conformément aux lois applicables.

Pour plus d'informations sur les exigences WhatsApp d'opt-in, voir Get Opt-in pour WhatsApp

Si les destinataires peuvent s'inscrire pour recevoir vos messages via un formulaire en ligne, empêchez les scripts automatisés d'inscrire des personnes à leur insu. Limitez également le nombre de fois qu'un utilisateur peut soumettre un numéro de téléphone au cours d'une même session.

Respectez toutes les demandes faites par une personne, qu'elle soit WhatsApp active ou non, visant à bloquer, interrompre ou refuser les communications, y compris en supprimant cette personne de votre liste de contacts.

Conservez les enregistrements incluant la date, l'heure et la source de chaque demande d'acceptation et de chaque confirmation. Cela peut également vous aider à effectuer des audits de routine de votre liste de clients.

Contenu de message interdit

⚠ Important

Travailler avec Meta/ WhatsApp

- Votre utilisation de la solution WhatsApp professionnelle est soumise aux conditions générales des conditions d'utilisation WhatsApp commerciales, aux conditions de la solution WhatsApp commerciale, à la politique de messagerie WhatsApp professionnelle, aux directives de WhatsApp messagerie et à toutes les autres conditions, politiques ou directives qui y sont incorporées par référence (car chacune peut être mise à jour de temps à autre).
- Méta ou WhatsApp peut à tout moment vous interdire l'utilisation de la solution WhatsApp commerciale.
- Dans le cadre de votre utilisation de la solution WhatsApp commerciale, vous ne soumettrez aucun contenu, information ou donnée soumis à des mesures de sauvegarde ou à des restrictions de distribution conformément aux lois ou réglementations applicables.

Si vous enfreignez cette WhatsApp politique, l'envoi de messages sur votre compte peut être bloqué pendant un certain temps, bloqué jusqu'à ce que vous déposiez un recours ou bloqué définitivement. Meta vous informera si l'un de vos comptes ou actifs a enfreint la politique, par e-mail et par le directeur WhatsApp commercial. Tous les appels doivent être adressés à Meta. Pour consulter une violation du règlement ou déposer un recours auprès de Meta, voir Afficher les détails de la violation de politique pour votre compte WhatsApp Business dans le centre d'aide de Meta Business. Pour obtenir la liste la plus récente des contenus de messages interdits, consultez la politique de messagerie WhatsApp professionnelle.

Les catégories de contenu suivantes sont interdites pour tous les types de messages dans le monde entier. Lorsque vous utilisez un service WhatsApp, vous pouvez utiliser les instructions suivantes :

Catégorie	Exemples
Jeu	• Casinos • Loteries promotionnelles • Applications/sites Web
Services financiers à haut risque	• Prêts sur salaire • Prêts à court terme et à taux d'intérêt élevé • Prêts automobiles • Prêts hypothécaires • Prêts étudiants • Recouvrement des créances • Alertes boursières • Crypto-monnaie
Annulation de la dette	• Consolidation des dettes • Réduction de la dette • Programmes de réparation de crédits
Get-rich-quick Scheme	• Work-from-home programmes • Opportunités d'investissement à faible risque • Schémas de marketing pyramidaux ou multi-niveaux

Catégorie	Exemples
Substances illégales	• Cannabis/CBD CBD
Hishing/Smishing	• Tentatives pour amener les utilisateurs à révéler des informations personnelles ou des informations de connexion au site Web.
S.H.A.F.T.	• Sexe • Haine • Alcool • Armes à feu • Tabac/vapotage
Génération de prospects par des tiers	• Entreprises qui achètent, vendent ou partagent des informations sur les consommateurs

Effectuer un audit de vos listes de clients

Si vous envoyez WhatsApp des messages récurrents, vérifiez régulièrement vos listes de clients. L'audit de vos listes de clients permet de vous assurer que les seuls clients qui reçoivent vos messages sont ceux qui souhaitent les recevoir.

Lorsque vous effectuez un audit de votre liste, envoyez à chaque client un message lui rappelant qu'il s'est abonné, et fournissez-lui les informations requises pour un désabonnement.

Ajuster votre envoi en fonction de l'implication

Les priorités de vos clients peuvent évoluer au fil du temps. Si les clients ne considèrent plus vos messages comme utiles, ils peuvent les refuser complètement, voire même les signaler comme messages indésirables. Pour ces raisons, il est important que vous ajustiez vos pratiques d'envoi en fonction de l'implication du client.

Pour les clients qui s'impliquent rarement par rapport à vos messages, vous devez ajuster la fréquence de ces derniers. Par exemple, si vous envoyez des messages hebdomadaires aux

clients impliqués, vous pouvez créer un récapitulatif mensuel distinct pour les clients qui sont moins impliqués.

Enfin, supprimez de vos listes de clients ceux qui ne sont pas impliqués du tout. Cette étape permet de prévenir toute frustration provoquée par vos messages de la part des clients. Elle vous permet d’économiser de l’argent et contribue à protéger votre réputation d’expéditeur.

Envoyer à des heures appropriées

Envoyez des messages uniquement pendant les heures normales d'ouverture de bureau. Si vous envoyez des messages à l'heure du dîner ou au milieu de la nuit, il y a de grandes chances que vos clients se désinscrivent de vos listes afin d'éviter d'être dérangés. Vous pouvez éviter d'envoyer WhatsApp des messages lorsque vos clients ne peuvent pas y répondre immédiatement.

Sécurité dans AWS la messagerie sociale des utilisateurs finaux

Chez, la sécurité du cloud AWS est notre priorité numéro 1. En tant que AWS client, vous bénéficiez de centres de données et d'architectures réseau conçus pour répondre aux exigences des organisations les plus pointilleuses en termes de sécurité.

La sécurité est une responsabilité partagée entre AWS et vous-même. Le modèle de responsabilité partagée décrit cela comme la sécurité du cloud et la sécurité dans le cloud :

- Sécurité du cloud — AWS est responsable de la protection de l'infrastructure qui exécute AWS les services dans le AWS Cloud. AWS AWS vous fournit également des services que vous pouvez utiliser en toute sécurité. Des auditeurs tiers testent et vérifient régulièrement l'efficacité de notre sécurité dans le AWS cadre des programmes de de . Pour en savoir plus sur les programmes de conformité qui s'appliquent à AWS la messagerie sociale pour les utilisateurs finaux, consultez AWS Services concernés par le programme de conformitéAWS .
- Sécurité dans le cloud — Votre responsabilité est déterminée par le AWS service que vous utilisez. Vous êtes également responsable d'autres facteurs, y compris de la sensibilité de vos données, des exigences de votre entreprise, ainsi que de la législation et de la réglementation applicables.

Cette documentation vous aide à comprendre comment appliquer le modèle de responsabilité partagée lors de l'utilisation de la messagerie sociale pour l'utilisateur AWS final. Les rubriques suivantes vous montrent comment configurer AWS End User Messaging Social pour répondre à vos objectifs de sécurité et de conformité. Vous pouvez également apprendre à utiliser d'autres AWS services qui vous aident à contrôler et sécuriser vos ressources de messagerie à l'utilisateur AWS final.

Rubriques

- Bonnes pratiques de sécurité
- Utilisation des rôles liés à un AWS service pour

Protection des données dans les réseaux sociaux destinés aux utilisateurs AWS finaux

Le modèle de responsabilité AWS partagée s'applique à la protection des données dans AWS End User Messaging Social. Comme décrit dans ce modèle, AWS est responsable de la protection de l'infrastructure globale sur laquelle l'ensemble AWS Cloud. La gestion du contrôle de votre contenu hébergé sur cette infrastructure relève de votre responsabilité. Vous êtes également responsable des tâches de configuration et de gestion de la sécurité des Services AWS que vous utilisez. Pour plus d'informations sur la confidentialité des données, veuillez consulter Politique de confidentialité des données FAQ. Pour plus d'informations sur la protection des données en Europe, consultez le billet de GDPR blog AWS Shared Responsibility Model in the AWS Security.

À des fins de protection des données, nous vous recommandons de protéger les Compte AWS informations d'identification et de configurer les comptes utilisateur individuels avec AWS IAM Identity Center ou AWS Identity and Access Management (IAM). Ainsi, chaque utilisateur se voit attribuer uniquement les autorisations nécessaires pour exécuter ses tâches. Nous vous recommandons également de sécuriser vos données comme indiqué ci-dessous :

- Utilisez l'authentification multifactorielle (MFAMFA) avec chaque compte.
- UtilisezSSL/TLSpour communiquer avec les AWS ressources. Nous exigeons TLS TLS 1.2 et recommandons TLS TLS 1.2.
- Configurez l'APIAPI et la journalisation des activités utilisateur avec AWS CloudTrail. Pour plus d'informations sur l'utilisation des CloudTrail sentiers pour capturer AWS des activités, consultez la section Utilisation des CloudTrail sentiers dans le guide de AWS CloudTrail l'utilisateur.
- Utilisez des solutions de AWS chiffrement, ainsi que tous les contrôles de sécurité par défaut au sein des Services AWS.
- Utilisez des services de sécurité gérés avancés tels qu'Amazon Macie, qui contribuent à la découverte et à la sécurisation des données sensibles stockées dans Amazon S3.
- Si vous avez besoin de FIPS 140 à 3 modules cryptographiques validés lorsque vous accédez à AWS via une interface de ligne de commande ou unAPI, utilisez un point de terminaison. FIPS Pour de plus amples informations sur les FIPS points de terminaison disponibles, consultez Federal Information Processing Standard (FIPS) 140-3.

Nous vous recommandons fortement de ne jamais placer d'informations confidentielles ou sensibles, telles que les adresses e-mail de vos clients, dans des balises ou des champs de texte libre tels que le champ Nom. Cela inclut lorsque vous travaillez avec AWS End User Messaging Social ou autre Services AWS à l'aide de la consoleAPI, AWS CLI, ou AWS SDKs. Toutes les données que vous entrez dans des balises ou des champs de texte de forme libre utilisés pour les noms peuvent être utilisées à des fins de facturation ou dans les journaux de diagnostic. Si vous fournissez un URL à un serveur externe, nous vous recommandons fortement de ne pas inclure d'informations d'identification dans le URL pour valider votre demande au serveur.

> **Important**
>
> WhatsApp utilise le protocole Signal pour des communications sécurisées. Toutefois, étant donné que AWS End User Messaging Social est une société tierce, ces messages WhatsApp ne sont pas considérés comme end-to-end chiffrés. Pour plus d'informations sur la protection WhatsApp des données, consultez le livre blanc « Présentation de la confidentialité, de la sécurité et du WhatsApp chiffrement des données ».

Chiffrement des données

AWS Messagerie à l'utilisateur final Les données sociales sont chiffrées en transit et au repos à l'intérieur des AWS limites. Lorsque vous soumettez des données à AWS End User Messaging Social, celles-ci sont chiffrées au fur et à mesure qu'elles sont reçues et les stocke. Lorsque vous récupérez des données AWS à partir de la messagerie sociale, celles-ci vous sont transmises à l'aide des protocoles de sécurité actuels.

Chiffrement au repos

AWS End User Messaging Social chiffre toutes les données qu'il stocke pour vous à l'intérieur de ces AWS limites. Cela inclut les données de configuration, les données d'enregistrement et toutes les données que vous ajoutez à AWS End User Messaging Social. Pour chiffrer vos données, AWS End User Messaging Social utilise des clés AWS Key Management Service (AWS KMS) internes, que le service possède et gère en votre nom. Pour des informations sur AWS KMS, consultez le guide du développeur AWS Key Management Service.

Chiffrement en transit

AWS Messagerie pour l'utilisateur final utilise HTTPS les réseaux sociaux et le protocole Transport Layer Security (TLS) 1.2 pour communiquer avec vos clients, vos applications et Meta. Pour

communiquer avec d'autres AWS services, AWS Final User Messaging Social utilise HTTPS et TLS 1.2. En outre, lorsque vous créez et gérez AWS SMS des ressources à l'aide de la console AWS SDK AWS Command Line Interface, toutes les communications sont sécurisées à l'aide de HTTPS et TLS 1.2.

Gestion des clés

Pour chiffrer vos données, AWS End User Messaging Social utilise des AWS KMS clés internes, que le service possède et gère en votre nom. Ces clés font l'objet d'une rotation régulière. Vous ne pouvez pas provisionner et utiliser vos propres clés AWS KMS ou d'autres clés pour chiffrer les données que vous stockez dans AWS .

Confidentialité du trafic inter-réseaux

La confidentialité du trafic inter-réseaux fait référence à la sécurisation des connexions et du trafic entre AWS End User Messaging Social et vos clients et applications sur site, ainsi qu'entre AWS End User Messaging Social et d'autres AWS ressources dans le même. Région AWS Les fonctionnalités et pratiques suivantes peuvent vous aider à garantir la confidentialité du trafic inter-réseaux pour la messagerie sociale de l'utilisateur AWS final.

Trafic entre AWS SMS et les clients et applications sur site

Pour établir une connexion privée entre AWS End User Messaging Social et des clients et des applications sur votre réseau sur site, vous pouvez utiliser AWS Direct Connect. Cela vous permet de relier votre réseau à un emplacement AWS Direct Connect à l'aide d'un câble Ethernet standard à fibre optique. Une extrémité du câble est connectée à votre routeur. L'autre extrémité est connectée à un AWS Direct Connect routeur. Pour plus d'informations, consultez Présentation d' AWS Direct Connect dans le Guide de l'utilisateur AWS Direct Connect .

Pour sécuriser l'accès à AWS la messagerie sociale de l'utilisateur final par le biais de la publicationAPIs, nous vous recommandons de respecter les exigences de messagerie sociale de l'utilisateur AWS final relatives aux API appels. AWS L'utilisateur final de Messaging Social exige que les clients utilisent Transport Layer Security (TLS) version 1.2 ou ultérieure. Les clients doivent également prendre en charge les suites de chiffrement avec une sécurité de transmission parfaite (PFS), comme Ephemeral Diffie-Hellman (DHE) ou Elliptic Curve Diffie-Hellman () ECDHE La plupart des systèmes modernes tels que Java 7 et les versions ultérieures prennent en charge ces modes.

En outre, les demandes doivent être signées à l'aide d'un ID de clé d'accès et d'une clé d'accès secrète associée à un principal AWS Identity and Access Management (IAM) pour votre AWS

compte. Vous pouvez également utiliser AWS Security Token Service (AWS STS) pour générer des informations d'identification de sécurité temporaires et signer les demandes.

Gestion des identités et des accès pour AWS Client Client Client Client Manager

AWS Identity and Access Management (IAM) est un outil Service AWS qui permet à un administrateur de contrôler en toute sécurité l'accès aux AWS ressources. IAMDes administrateurs contrôlent les personnes qui s'authentifient (sont connectées) et sont autorisées (disposent d'autorisations) à utiliser des ressources sociales de messagerie pour utilisateurs AWS finaux. IAMIAM est un service Service AWS que vous pouvez utiliser sans frais supplémentaires.

Rubriques

Public ciblé

Votre utilisation d' AWS Identity and Access Management (IAM) diffère selon la tâche que vous AWS accomplissez dans.

Utilisateur du service : si vous utilisez le service social de messagerie utilisateur AWS final pour effectuer votre tâche, votre administrateur vous fournit les informations d'identification et les autorisations dont vous avez besoin. Plus vous utiliserez de fonctionnalités sociales de messagerie pour l'utilisateur AWS final pour effectuer votre tâche, plus vous pourriez avoir besoin d'autorisations supplémentaires. En comprenant bien la gestion des accès, vous saurez demander les autorisations appropriées à votre administrateur. Si vous ne pouvez pas accéder à une fonctionnalité dans AWS End User Messaging Social, veuillez consulterRésolution des problèmes liés AWS à l'identité et à l'accès aux réseaux sociaux des utilisateurs finaux.

Administrateur du service — Si vous êtes le responsable des AWS ressources sociales de votre entreprise, vous bénéficiez probablement d'un accès total à AWS End User Messaging Social. Votre responsabilité est de déterminer les fonctionnalités et les ressources sociales auxquelles AWS les utilisateurs de votre service doivent accéder. Vous devez ensuite soumettre les demandes à votre IAM administrateur pour modifier les autorisations des utilisateurs de votre service. Consultez les informations sur cette page pour comprendre les concepts de base d'IAM. Pour en savoir plus sur la façon dont votre entreprise peut utiliser IAM AWS Final User Messaging Social, consultezComment fonctionne AWS Final User Messaging Social IAM.

IAMadministrateur : si vous êtes un IAM administrateur, vous souhaiterez peut-être en savoir plus sur la façon d'écrire des stratégies pour gérer l'accès à AWS End User Messaging Social. Pour voir AWS des exemples de stratégies basées sur l'identité sociale dansIAM. Exemples de politiques basées sur l'identité pour AWS Amazon Airposts

Authentification par des identités

L'authentification correspond au processus par lequel vous vous AWS connectez à avec vos informations d'identification. Vous devez être authentifié (connecté à AWS) en tant que Utilisateur racine d'un compte AWS, en tant qu'IAMutilisateur ou en assumant un IAM rôle.

Vous pouvez vous connecter à en AWS tant qu'identité fédérée à l'aide des informations d'identification fournies par le biais d'une source d'identité. AWS IAM Identity Center Les utilisateurs (IAMIdentity Center), l'authentification de connexion unique de votre entreprise et vos informations d'identification Google ou Facebook sont des exemples d'identités fédérées. Lorsque vous vous connectez en tant qu'identité fédérée, votre administrateur aura précédemment configuré une fédération d'identités avec IAM des rôles. Lorsque vous accédez à AWS en utilisant la fédération, vous endossez indirectement un rôle.

Selon le type d'utilisateur que vous êtes, vous pouvez vous connecter à la AWS Management Console ou au portail AWS d'accès. Pour plus d'informations sur la connexion à AWS, consultez la section Comment vous connecter à votre compte Compte AWS dans le guide de Connexion à AWS l'utilisateur.

Si vous accédez à AWS par programmation, AWS fournit un kit de développement logiciel (SDK) et une interface de ligne de commande (CLI) pour signer cryptographiquement vos demandes en utilisant vos informations d'identification. Si vous n'utilisez pas AWS les outils, vous devez signer la requête vous-même. Pour plus d'informations sur l'utilisation de la méthode recommandée pour signer des demandes vous-même, consultez Signature des AWS API demandes dans le Guide de IAM l'utilisateur.

Quelle que soit la méthode d'authentification que vous utilisez, vous devrez peut-être fournir des informations de sécurité supplémentaires. Par exemple, vous AWS recommande d'utiliser l'authentification multifactorielle (MFA) pour améliorer la sécurité de votre compte. Pour en savoir plus, consultez Authentification multifactorielle dans le guide de AWS IAM Identity Center l'utilisateur et Utilisation de l'authentification multifactorielle (MFA) AWS dans le guide de l'IAMutilisateur.

Compte AWS Utilisateur racine racine racine.

Lorsque vous créez un Compte AWS, vous commencez avec une seule identité de connexion disposant d'un accès complet à tous les Services AWS et ressources du compte. Cette identité est appelée l'utilisateur Compte AWS racine du. Vous pouvez y accéder en vous connectant à l'aide de l'adresse e-mail et du mot de passe que vous avez utilisés pour créer le compte. Il est vivement recommandé de ne pas utiliser l'utilisateur racine pour vos tâches quotidiennes. Protégez vos informations d'identification d'utilisateur racine et utilisez-les pour effectuer les tâches que seul l'utilisateur racine peut effectuer. Pour obtenir la liste complète des tâches qui vous imposent de vous connecter en tant qu'utilisateur root, consultez Tâches nécessitant des informations d'identification d'utilisateur root dans le Guide de IAM l'utilisateur.

Identité fédérée

Demandez aux utilisateurs humains, et notamment aux utilisateurs qui nécessitent un accès administrateur, d'appliquer la bonne pratique consistant à utiliser une fédération avec fournisseur d'identité pour accéder à en Services AWS utilisant des informations d'identification temporaires.

Une identité fédérée est un utilisateur de l'annuaire des utilisateurs de votre entreprise, un fournisseur d'identité Web AWS Directory Service, l'annuaire Identity Center ou tout utilisateur qui accède à en Services AWS utilisant des informations d'identification fournies via une source d'identité. Lorsque des identités fédérées accèdent à Comptes AWS, elles assument des rôles, ces derniers fournissant des informations d'identification temporaires.

Pour une gestion des accès centralisée, nous vous recommandons d'utiliser AWS IAM Identity Center. Vous pouvez créer des utilisateurs et des groupes dans IAM Identity Center, ou vous connecter et vous synchroniser avec un ensemble d'utilisateurs et de groupes dans votre propre source d'identité pour une utilisation sur l'ensemble de vos applications Comptes AWS et de vos. Pour plus d'informations sur IAM Identity Center, consultez Qu'est-ce qu'IAMIdentity Center ? dans le guide de AWS IAM Identity Center l'utilisateur.

Utilisateurs et groupes IAM

Un IAMutilisateur est une identité dans votre identité Compte AWS qui dispose d'autorisations spécifiques pour une seule personne ou application. Dans la mesure du possible, nous vous recommandons de vous appuyer sur des informations d'identification temporaires plutôt que de créer des IAM utilisateurs ayant des informations d'identification à long terme tels que les clés d'accès. Toutefois, si certains cas d'utilisation spécifiques nécessitent des informations d'identification à long terme avec IAM les utilisateurs, nous vous recommandons de faire pivoter les clés d'accès. Pour plus d'informations, veuillez consulter Rotation régulière des clés d'accès pour les cas d'utilisation nécessitant des informations d'identification dans le Guide de IAM l'utilisateur.

Un IAMgroupe est une identité qui définit un ensemble d'IAMutilisateurs. Vous ne pouvez pas vous connecter en tant que groupe. Vous pouvez utiliser les groupes pour spécifier des autorisations pour plusieurs utilisateurs à la fois. Les groupes permettent de gérer plus facilement les autorisations pour de grands ensembles d'utilisateurs. Par exemple, vous pouvez avoir un groupe nommé IAMAdminset accorder à ce groupe les autorisations leur permettant d'administrer IAM des ressources.

Les utilisateurs sont différents des rôles. Un utilisateur est associé de manière unique à une personne ou une application, alors qu'un rôle est conçu pour être endossé par tout utilisateur qui en a besoin. Les utilisateurs disposent d'informations d'identification permanentes, mais les rôles fournissent des informations d'identification temporaires. Pour en savoir plus, voir Quand créer un IAM utilisateur (au lieu d'un rôle) dans le Guide de IAM l'utilisateur.

IAMrôles

Un IAMrôle est une identité au sein de Compte AWS vous dotée d'autorisations spécifiques. Le concept ressemble à celui d'un IAM utilisateur, mais un rôle n'est pas associé à une personne en particulier. Vous pouvez temporairement endosser un IAM rôle dans la en AWS Management Console changeant de rôle. Vous pouvez assumer un rôle en appelant une AWS API opération AWS CLI or ou en utilisant une option personnaliséeURL. Pour plus d'informations sur les méthodes d'utilisation des rôles, consultez la section Méthodes pour assumer un rôle dans le Guide de IAM l'utilisateur.

IAMLes rôles avec des informations d'identification temporaires sont utiles dans les cas suivants :

- Accès utilisateur fédéré : pour attribuer des autorisations à une identité fédérée, vous créez un rôle et définissez des autorisations pour le rôle. Quand une identité externe s'authentifie, l'identité est associée au rôle et reçoit les autorisations qui sont définies par celui-ci. Pour plus d'informations sur les rôles pour la fédération, voir Création d'un rôle pour un fournisseur d'identité

tiers dans le guide de IAM l'utilisateur. Si vous utilisez IAM Identity Center, vous configurez un jeu d'autorisations. Pour contrôler à quoi vos identités peuvent accéder après leur authentification, IAM Identity Center met en corrélation le jeu d'autorisations avec un rôle dans. IAM Pour plus d'informations sur les jeux d'autorisations, consultez Jeux d'autorisations dans le Guide de l'utilisateur AWS IAM Identity Center .

- Autorisations IAM utilisateur temporaires : un IAM utilisateur ou un rôle peut IAM endosser un rôle pour accepter différentes autorisations temporaires concernant une tâche spécifique.
- Accès intercompte : vous pouvez utiliser un IAM rôle pour permettre à un utilisateur (un principal de confiance) d'un compte différent d'accéder aux ressources de votre compte. Les rôles constituent le principal moyen d'accorder l'accès intercompte. Toutefois Services AWS, certains vous permettent d'attacher une politique directement à une ressource (au lieu d'utiliser un rôle en tant que proxy). Pour en savoir plus sur la différence entre les rôles et les politiques basées sur les ressources pour l'accès intercompte, consultez Accès intercompte aux ressources IAM dans le Guide de l'IAMutilisateur.
- Accès interservices : certains Services AWS utilisent des fonctionnalités dans d'autres Services AWS. Par exemple, lorsque vous effectuez un appel dans un service, il est courant que ce service exécute des applications dans Amazon EC2 ou stocke des objets dans Amazon S3. Un service peut le faire en utilisant les autorisations d'appel du principal, un rôle de service ou un rôle lié au service.
  - Transmission de sessions d'accès (FAS) : lorsque vous vous servez IAM d'un utilisateur ou d'un rôle pour effectuer des actions dans AWS, vous êtes considéré comme principal. Lorsque vous utilisez certains services, vous pouvez effectuer une action qui initie une autre action dans un autre service. FASutilise les autorisations du principal qui appelle Service AWS, combinées Service AWS à qui demande pour effectuer des demandes aux services en aval. FASles demandes ne sont effectuées que lorsqu'un service reçoit une demande dont l'exécution nécessite des interactions avec d'autres Services AWS ou ressources. Dans ce cas, vous devez disposer d'autorisations nécessaires pour effectuer les deux actions. Pour plus de détails sur la politique relative à la transmission de FAS demandes, consultez la section Sessions de transmission d'accès.
  - Fonction du service : il s'agit d'une fonction attribuée à un IAMrôle afin de réaliser des actions dans votre compte en votre nom. Un IAM administrateur peut créer, modifier et supprimer une fonction du service à partir de l'IAM. Pour plus d'informations, consultez la section Création d'un rôle auquel déléguer des autorisations Service AWS dans le Guide de IAM l'utilisateur.
  - Rôle lié au service — Un rôle lié au service est un type de rôle de service lié à un. Service AWS Le service peut endosser le rôle afin d'effectuer une action en votre nom. Les rôles

liés à un service s'affichent dans votre Compte AWS et sont détenus par le service. Un IAM administrateur peut consulter, mais ne peut pas modifier, les autorisations concernant les rôles liés à un service.

- Applications exécutées sur Amazon EC2 : vous pouvez utiliser un IAM rôle pour gérer les informations d'identification temporaires pour les applications qui s'exécutent sur une EC2 instance et qui font AWS CLI des AWS API demandes. Cette solution est préférable au stockage des clés d'accès au sein de l'EC2instance principale. Pour attribuer un AWS rôle à une EC2 instance et le rendre disponible pour toutes les applications associées, vous pouvez créer un profil d'instance attaché à l'instance. Un profil d'instance contient le rôle et permet aux programmes qui s'exécutent sur l'EC2instance d'obtenir des informations d'identification temporaires. Pour plus d'informations, consultez la section Utilisation d'un IAM rôle pour accorder des autorisations aux applications exécutées sur des EC2 instances Amazon dans le Guide de IAM l'utilisateur.

Pour savoir s'il faut utiliser IAM des rôles ou des IAM utilisateurs, voir Quand créer un IAM rôle (au lieu d'un utilisateur) dans le guide de IAM l'utilisateur.

Gestion des accès à l'aide de politiques

Vous contrôlez les accès dans en AWS créant des stratégies et en les attachant à AWS des identités ou à des ressources. Une stratégie est un objet dans AWS qui, lorsqu'il est associé à une identité ou à une ressource, définit ses autorisations. AWS évalue ces politiques lorsqu'un principal (utilisateur, racine ou session de rôle) envoie une demande. Les autorisations dans les politiques déterminent si la demande est autorisée ou refusée. La plupart des stratégies sont stockées dans en AWS tant que JSON documents JSON. Pour plus d'informations sur la structure et le contenu des documents de JSON stratégie, veuillez consulter Présentation des JSON stratégies dans le Guide de IAM l'utilisateur.

Les administrateurs peuvent utiliser AWS JSON les stratégies pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

Par défaut, les utilisateurs et les rôles ne disposent d'aucune autorisation. Pour octroyer aux utilisateurs des autorisations d'effectuer des actions sur les ressources dont ils ont besoin, un IAM administrateur peut créer des IAM politiques. L'administrateur peut ensuite ajouter les IAM politiques aux rôles et les utilisateurs peuvent assumer les rôles.

IAMLes stratégies définissent les autorisations d'une action quelle que soit la méthode que vous utilisez pour exécuter l'opération. Par exemple, supposons que vous disposiez d'une politique qui

autorise l'action `iam:GetRole`. Un utilisateur doté de cette politique peut obtenir des informations sur le rôle auprès du AWS Management Console AWS CLI, ou du AWS API.

Politiques basées sur l'identité

Les stratégies basées sur l'identité sont JSON des documents de stratégie d'autorisations que vous pouvez attacher à une identité telle qu'un IAM utilisateur, un groupe d'utilisateurs ou un rôle. Ces politiques contrôlent quel type d'actions des utilisateurs et des rôles peuvent exécuter, sur quelles ressources et dans quelles conditions. Pour découvrir comment créer une stratégie basée sur l'identité, veuillez consulter Création de IAM stratégies dans le Guide de l'IAMutilisateur.

Les politiques basées sur l'identité peuvent être classées comme des politiques en ligne ou des politiques gérées. Les politiques en ligne sont intégrées directement à un utilisateur, groupe ou rôle. Les politiques gérées sont des politiques autonomes que vous pouvez lier à plusieurs utilisateurs, groupes et rôles dans votre Compte AWS. Les stratégies gérées incluent les stratégies AWS gérées par et les stratégies gérées par le client. Pour découvrir comment choisir entre une politique gérée et une politique en ligne, veuillez consulter Choix entre les stratégies gérées et les stratégies en ligne dans le Guide de l'IAMutilisateur.

Politiques basées sur les ressources

Les politiques basées sur les ressources sont des documents JSON de politique que vous attachez à une ressource. Des stratégies basées sur les ressources sont par exemple, les stratégies de confiance de IAM rôle et des stratégies de compartiment Amazon S3. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour contrôler l'accès à une ressource spécifique. Pour la ressource dans laquelle se trouve la politique, cette dernière définit quel type d'actions un principal spécifié peut effectuer sur cette ressource et dans quelles conditions. Vous devez spécifier un principal dans une politique basée sur les ressources. Les mandataires peuvent inclure des comptes, des comptes, des rôles, des comptes, des comptes, des comptes, des comptes, des comptes, des comptes, des Services AWS

Les politiques basées sur les ressources sont des politiques en ligne situées dans ce service. Vous ne pouvez pas utiliser les stratégies AWS gérées IAM à partir d'une politique basée sur une ressource.

Listes de contrôle d'accès (ACLACLs) dans

Les listes de contrôle d'accès (ACLs) vérifient quels principaux (membres de compte, utilisateurs ou rôles) ont l'autorisation d'accéder à une ressource. ACLssont similaires aux politiques basées sur les ressources, bien qu'elles n'utilisent pas le format de document JSON de stratégie.

Amazon S3 et Amazon VPC sont des exemples de services compatiblesACLs. AWS WAF Pour en savoir plusACLs, consultez Présentation de la liste de contrôle d'accès (ACL) dans le Guide du développeur Amazon Simple Storage Service.

Autres types de politique

AWS prend en charge d'autres types de stratégies moins courantes. Ces types de politiques peuvent définir le nombre maximum d'autorisations qui vous sont accordées par des types de politiques plus courants.

- Limite d'autorisations : une limite d'autorisations est une fonctionnalité avancée dans laquelle vous définissez le nombre maximal d'autorisations qu'une politique basée sur l'identité peut accorder à une IAM entité (IAMutilisateur ou rôle). Vous pouvez définir une limite d'autorisations pour une entité. Les autorisations en résultant représentent la combinaison des politiques basées sur l'identité d'une entité et de ses limites d'autorisation. Les politiques basées sur les ressources qui spécifient l'utilisateur ou le rôle dans le champ `Principal` ne sont pas limitées par les limites d'autorisations. Un refus explicite dans l'une de ces politiques annule l'autorisation. Pour de plus amples informations sur les limites d'autorisations, veuillez consulter Limites d'autorisations pour IAM des entités dans le Guide de IAM l'utilisateur.
- Stratégies de contrôle de service (SCPs) : SCPs sont des JSON stratégies qui spécifient les autorisations maximales pour une organisation ou une unité d'organisation (UO) dans AWS Organizations. AWS Organizations est un service permettant de regrouper et de gérer de façon centralisée plusieurs Comptes AWS détenus par votre entreprise. Si vous activez toutes les fonctions d'une organisation, vous pouvez appliquer les stratégies de contrôle de service (SCPs) à l'un ou à l'ensemble de vos comptes. Les SCP limites d'autorisations pour les entités dans les comptes membres, y compris dans chaque Utilisateur racine d'un compte AWS. Pour plus d'informations sur les Organizations et consultez SCPs les politiques de contrôle des services dans le Guide de AWS Organizations l'utilisateur.
- Politiques de séance : les politiques de séance sont des politiques avancées que vous utilisez en tant que paramètre lorsque vous créez par programmation une séance temporaire pour un rôle ou un utilisateur fédéré. Les autorisations de séance en résultant sont une combinaison des politiques basées sur l'identité de l'utilisateur ou du rôle et des politiques de séance. Les autorisations peuvent également provenir d'une politique basée sur les ressources. Un refus explicite dans l'une de ces politiques annule l'autorisation. Pour plus d'informations, consultez la section Politiques de session dans le guide de IAM l'utilisateur.

Plusieurs types de politique

Lorsque plusieurs types de politiques s’appliquent à la requête, les autorisations en résultant sont plus compliquées à comprendre. Pour découvrir la façon dont AWS détermine s'il convient d'autoriser une demande en présence de plusieurs types de stratégies, consultez Logique d'évaluation de stratégies dans le Guide de IAM l'utilisateur.

Comment fonctionne AWS Final User Messaging Social IAM

Avant de commencer IAM à gérer l'accès à AWS End User Messaging Social, découvrez quelles IAM fonctionnalités peuvent être utilisées avec AWS End User Messaging Social.

IAMfonctionnalités que vous pouvez utiliser avec AWS End User Messaging Social

IAMfonctionnalité	AWS Messagerie à l'utilisateur final Assistance sociale
Politiques basées sur l’identité	Oui
Politiques basées sur les ressources	Non
Actions de politique	Oui
Ressources de politique	Oui
Clés de condition de politique	Oui
ACLs	Non
ABAC(balises dans les politiques)	Partielle
Informations d’identification temporaires	Oui
Autorisations de principal	Oui
Rôles de service	Oui
Rôles liés à un service	Oui

Pour obtenir une vue d'ensemble de la façon AWS dont les services de messagerie et d'autres AWS services fonctionnent avec la plupart des IAM fonctions, consultez AWS Services qui fonctionnent avec IAM dans le Guide de IAM l'utilisateur.

Politiques basées sur l'identité pour AWS Amazon Airposts

Prend en charge les politiques basées sur l’identité : oui

Les stratégies basées sur l'identité sont JSON des documents de stratégie d'autorisations que vous pouvez attacher à une identité telle qu'un IAM utilisateur, un groupe d'utilisateurs ou un rôle. Ces politiques contrôlent quel type d’actions des utilisateurs et des rôles peuvent exécuter, sur quelles ressources et dans quelles conditions. Pour découvrir comment créer une stratégie basée sur l'identité, veuillez consulter Création de IAM stratégies dans le Guide de l'IAMutilisateur.

Avec les politiques IAM basées sur l'identité, vous pouvez spécifier des actions et ressources autorisées ou refusées, ainsi que les conditions dans lesquelles les actions sont autorisées ou refusées. Vous ne pouvez pas spécifier le principal dans une politique basée sur une identité, car celle-ci s’applique à l’utilisateur ou au rôle auquel elle est attachée. Pour en savoir plus sur tous les éléments que vous pouvez utiliser dans une JSON politique, consultez la référence aux éléments de IAM JSON politique dans le Guide de IAM l'utilisateur.

Exemples de politiques basées sur l'identité pour AWS Amazon Airposts

Pour voir des exemples AWS de politiques basées sur l'identité, veuillez consulter. Exemples de politiques basées sur l'identité pour AWS Amazon Airposts

Politiques basées sur une ressource dans Elastic AWS Load Balance

Prend en charge les politiques basées sur les ressources : non

Les politiques basées sur les ressources sont des documents JSON de politique que vous attachez à une ressource. Des stratégies basées sur les ressources sont par exemple, les stratégies de confiance de IAM rôle et des stratégies de compartiment Amazon S3. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour contrôler l’accès à une ressource spécifique. Pour la ressource dans laquelle se trouve la politique, cette dernière définit quel type d’actions un principal spécifié peut effectuer sur cette ressource et dans quelles conditions. Vous devez spécifier un principal dans une politique basée sur les ressources. Les mandataires peuvent inclure des comptes, des comptes, des rôles, des comptes, des comptes, des comptes, des comptes, des comptes, des comptes, des Services AWS

Pour permettre un accès intercompte, vous pouvez spécifier un compte entier ou IAM des entités dans un autre compte en tant que principal dans une stratégie basée sur les ressources. L'ajout d'un principal entre comptes à une politique basée sur les ressources ne représente qu'une partie de l'instauration de la relation d'approbation. Quand le mandataire et la ressource se trouvent dans des différents Comptes AWS, un IAM administrateur du compte approuvé doit également accorder à l'entité principal (utilisateur ou rôle) l'autorisation d'accéder à la ressource. Pour ce faire, il attache une politique basée sur une identité à l'entité. Toutefois, si une politique basée sur des ressources accorde l'accès à un principal dans le même compte, aucune autre politique basée sur l'identité n'est requise. Pour plus d'informations, consultez la section Accès aux ressources entre comptes IAM dans le Guide de IAM l'utilisateur.

Actions stratégiques pour la messagerie sociale destinée aux utilisateurs AWS finaux

Prend en charge les actions de politique : oui

Les administrateurs peuvent utiliser AWS JSON les stratégies pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'`Action`élément d'une JSON stratégie décrit les actions que vous pouvez utiliser pour autoriser ou refuser l'accès à une stratégie. Les actions de stratégie possèdent généralement le même nom que l' AWS APIopération associée. Il existe quelques exceptions, telles que les actions avec autorisations uniquement qui n'ont pas d'opération correspondante. API Certaines opérations nécessitent également plusieurs actions dans une politique. Ces actions supplémentaires sont nommées actions dépendantes.

Intégration d'actions dans une politique afin d'accorder l'autorisation d'exécuter les opérations associées.

Pour consulter la liste des actions de messagerie sociale de l'utilisateur AWS final, consultez la section Actions définies par l'utilisateur AWS final de Messaging Social dans la référence d'autorisation du service.

Les actions de stratégie dans AWS End User Messaging Social utilisent le préfixe suivant avant l'action :

```
social-messaging
```

Pour indiquer plusieurs actions dans une seule déclaration, séparez-les par des virgules.

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

Pour voir des exemples AWS de politiques basées sur l'identité, veuillez consulter. Exemples de politiques basées sur l'identité pour AWS Amazon Airposts

Ressources relatives aux politiques relatives à AWS la messagerie sociale destinée aux utilisateurs finaux

Prend en charge les ressources de politique : oui

Les administrateurs peuvent utiliser AWS JSON les stratégies pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément `Resource` JSON de stratégie spécifie le ou les objets auxquels l'action s'applique. Les instructions doivent inclure un élément `Resource` ou `NotResource`. Il est recommandé de définir une ressource à l'aide de son Amazon Resource Name (ARN). Vous pouvez le faire pour des actions qui prennent en charge un type de ressource spécifique, connu sous la dénomination autorisations de niveau ressource.

Pour les actions qui ne sont pas compatibles avec les autorisations de niveau ressource, telles que les opérations de liste, utilisez un caractère générique (*) afin d'indiquer que l'instruction s'applique à toutes les ressources.

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

Pour consulter la liste des types de ressources sociales de messagerie destinés aux utilisateurs AWS finaux et leurs caractéristiquesARNs, consultez la section Ressources définies par AWS End User Messaging Social dans la référence d'autorisation de service. Pour savoir grâce à quelles actions vous pouvez spécifier pour chaque ressource, consultez Actions définies par l'utilisateur AWS final Messaging Social. ARN

Pour voir des exemples AWS de politiques basées sur l'identité, veuillez consulter. Exemples de politiques basées sur l'identité pour AWS Amazon Airposts

Clés de condition de AWS politique pour SGW

Prend en charge les clés de condition de politique spécifiques au service : oui

Les administrateurs peuvent utiliser AWS JSON les stratégies pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément `Condition` (ou le bloc `Condition`) vous permet de spécifier des conditions lorsqu'une instruction est appliquée. L'élément `Condition` est facultatif. Vous pouvez créer des expressions conditionnelles qui utilisent des opérateurs de condition, tels que les signes égal ou inférieur à, pour faire correspondre la condition de la politique aux valeurs de la demande.

Si vous spécifiez plusieurs éléments `Condition` dans une instruction, ou plusieurs clés dans un seul élément `Condition`, AWS les évalue à l'aide d'une opération `AND` logique. Si vous spécifiez plusieurs valeurs pour une seule clé de condition, AWS évalue la condition à l'aide d'une `OR` opération logique. Toutes les conditions doivent être remplies avant que les autorisations associées à l'instruction ne soient accordées.

Vous pouvez aussi utiliser des variables d'espace réservé quand vous spécifiez des conditions. Par exemple, vous pouvez accorder à un IAM utilisateur l'autorisation d'accéder à une ressource uniquement si elle est balisée avec son nom IAM d'utilisateur. Pour plus d'informations, consultez IAMla section Éléments de politique : variables et balises dans le Guide de IAM l'utilisateur.

AWS prend en charge les clés de condition globales et les clés de condition spécifiques à un service. Pour afficher toutes les clés de condition AWS globales, veuillez consulter Clés de contexte de condition AWS globales dans le Guide de IAM l'utilisateur.

Pour consulter la liste des clés de condition sociale de messagerie utilisateur AWS final, voir Clés de condition pour AWS la messagerie sociale de l'utilisateur final dans la référence d'autorisation de service. Pour savoir avec quelles actions et ressources vous pouvez utiliser une clé de condition, consultez Actions définies par l'utilisateur AWS final Messaging Social.

Pour voir des exemples AWS de politiques basées sur l'identité, veuillez consulter. Exemples de politiques basées sur l'identité pour AWS Amazon Airposts

ACLsMessagerie sociale pour les utilisateurs AWS finaux

Supports ACLs : Non

Les listes de contrôle d'accès (ACLs) vérifient quels principaux (membres de compte, utilisateurs ou rôles) ont l'autorisation d'accéder à une ressource. ACLssont similaires aux politiques basées sur les ressources, bien qu'elles n'utilisent pas le format de document JSON de stratégie.

ABACavec AWS Final User Messaging Social

Supports ABAC (balises dans les politiques) : Partiel

Le contrôle d'accès basé sur les attributs (ABAC) est une stratégie d'autorisation qui définit les autorisations en fonction des attributs. Dans AWS, ces attributs sont appelés balises. Vous pouvez attacher des balises à IAM des entités (utilisateurs ou rôles) et à de nombreuses AWS ressources. L'authentification est la première étape d'ABACABAC. Vous concevez ensuite des ABAC politiques pour autoriser des opérations quand l'identification du principal correspond à celle de la ressource à laquelle il tente d'accéder.

ABACest utile dans les environnements qui connaissent une croissance rapide et pour les cas où la gestion des stratégies devient fastidieuse.

Pour contrôler l'accès basé sur des étiquettes, vous devez fournir les informations d'étiquette dans l'élément de condition d'une politique utilisant les clés de condition `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` ou `aws:TagKeys`.

Si un service prend en charge les trois clés de condition pour tous les types de ressources, alors la valeur pour ce service est Oui. Si un service prend en charge les trois clés de condition pour certains types de ressources uniquement, la valeur est Partielle.

Pour plus d'informationsABAC, voir Qu'est-ce que c'est ABAC ? dans le guide de IAM l'utilisateur. Pour consulter un didacticiel présentant les étapes de configurationABAC, voir Utiliser le contrôle d'accès basé sur les attributs (ABAC) dans le guide de l'IAMutilisateur.

Utilisation des informations d'identification AWS temporaires avec Amazon Mail

Prend en charge les informations d'identification temporaires : oui

Certains services Services AWS ne fonctionnent pas quand vous vous connectez à l'aide d'informations d'identification temporaires. Pour plus d'informations, y compris celles qui Services

AWS fonctionnent avec des informations d'identification temporaires, consultez Services AWS la section relative à l'utilisation IAM dans le Guide de IAM l'utilisateur.

Vous utilisez des informations d'identification temporaires si vous vous connectez à la en AWS Management Console utilisant toute méthode autre qu'un nom d'utilisateur et un mot de passe. Par exemple, lorsque vous accédez à AWS en utilisant le lien d'authentification unique (SSO) de votre société, ce processus crée automatiquement des informations d'identification temporaires. Vous créez également automatiquement des informations d'identification temporaires lorsque vous vous connectez à la console en tant qu'utilisateur, puis changez de rôle. Pour plus d'informations sur le changement de rôle, consultez la section Passage à un rôle (console) dans le guide de IAM l'utilisateur.

Vous pouvez créer manuellement des informations d'identification temporaires à l'aide de AWS CLI ou AWS API. Vous pouvez ensuite utiliser ces informations d'identification temporaires pour y accéder AWS. AWS vous recommande de générer des informations d'identification temporaires de façon dynamique au lieu d'utiliser des clés d'accès à long terme. Pour plus d'informations, consultez Informations d'identification de sécurité temporaires dans IAM.

Autorisations du principal entre services pour AWS Elastic Load Balancement

Prend en charge les sessions d'accès direct (FASFAS) :

Lorsque vous vous servez d'un IAM utilisateur ou d'un rôle pour accomplir des actions dans AWS, vous êtes considéré comme mandataire. Lorsque vous utilisez certains services, vous pouvez effectuer une action qui initie une autre action dans un autre service. FASutilise les autorisations du principal qui appelle Service AWS, combinées Service AWS à qui demande pour effectuer des demandes aux services en aval. FASles demandes ne sont effectuées que lorsqu'un service reçoit une demande dont l'exécution nécessite des interactions avec d'autres Services AWS ou ressources. Dans ce cas, vous devez disposer d'autorisations nécessaires pour effectuer les deux actions. Pour plus de détails sur la politique relative à la transmission de FAS demandes, consultez la section Sessions de transmission d'accès.

Rôles de service pour l'utilisateur AWS final Messaging Social

Prend en charge les rôles de service : oui

Une fonction de service est un IAMrôle qu'un service endosse pour accomplir des actions en votre nom. Un IAM administrateur peut créer, modifier et supprimer une fonction du service à partir de l'IAM. Pour plus d'informations, consultez la section Création d'un rôle auquel déléguer des autorisations Service AWS dans le Guide de IAM l'utilisateur.

> **Warning**
>
> Le fait de changer les autorisations d'une fonction du service peut altérer AWS la fonctionnalité de messagerie pour les utilisateurs finaux. Évitez de modifier les fonctions du service si vous n'y êtes pas invité par AWS End User Messaging Social.

Rôles liés à un service pour l'utilisateur AWS final Messaging Social

Prend en charge les rôles liés aux services : Oui

Un rôle lié à un service est un type de fonction du service lié à un. Service AWS Le service peut endosser le rôle afin d'effectuer une action en votre nom. Les rôles liés à un service s'affichent dans votre Compte AWS et sont détenus par le service. Un IAM administrateur peut consulter, mais ne peut pas modifier, les autorisations concernant les rôles liés à un service.

Pour plus d'informations sur la création ou la gestion des rôles liés à un service, consultez AWS Services qui fonctionnent avec. IAM Recherchez un service dans le tableau qui inclut un `Yes` dans la colonne Rôle lié à un service. Choisissez le lien Oui pour consulter la documentation du rôle lié à ce service.

Exemples de politiques basées sur l'identité pour AWS Amazon Airposts

Par défaut, les utilisateurs et les rôles ne disposent pas des autorisations nécessaires pour créer ou AWS modifier des ressources sociales de messagerie. Ils ne peuvent pas non plus effectuer de tâches en utilisant le AWS Management Console, AWS Command Line Interface (AWS CLI) ou AWS API. Pour octroyer aux utilisateurs des autorisations d'effectuer des actions sur les ressources dont ils ont besoin, un IAM administrateur peut créer des IAM politiques. L'administrateur peut ensuite ajouter les IAM politiques aux rôles et les utilisateurs peuvent assumer les rôles.

Pour savoir comment créer une politique IAM basée sur l'identité à l'aide de ces exemples de documents de JSON stratégie, consultez la section Création de IAM politiques dans le guide de l'IAMutilisateur.

Pour plus de détails sur les actions et les types de ressources définis par AWS End User Messaging Social, y compris le format de ARNs pour chacun des types de ressources, consultez Actions, ressources et clés de condition pour l'utilisateur AWS final Messaging Social dans la Référence de l'autorisation de service.

Rubriques

- Bonnes pratiques en matière de politiques
- Utilisation de la console sociale de messagerie utilisateur AWS final
- Autorisation accordée aux utilisateurs pour afficher leurs propres autorisations

Bonnes pratiques en matière de politiques

Les politiques basées sur l'identité déterminent si une personne peut créer, consulter ou supprimer des ressources de messagerie pour les utilisateurs AWS finaux dans votre compte. Ces actions peuvent entraîner des frais pour votre Compte AWS. Lorsque vous créez ou modifiez des politiques basées sur l'identité, suivez ces instructions et recommandations :

- Commencez AWS par les politiques gérées et passez aux autorisations relatives au moindre privilège : pour commencer à accorder des autorisations à vos utilisateurs et charges de travail, utilisez les stratégies AWS gérées qui accordent des autorisations pour de nombreux cas d'utilisation courants. Ils sont disponibles dans votre Compte AWS. Nous vous recommandons de réduire encore les autorisations en définissant des politiques gérées par le AWS client qui sont spécifiques à vos cas d'utilisation. Pour plus d'informations, consultez les politiques AWS gérées ou les politiques AWS gérées pour les fonctions professionnelles dans le Guide de IAM l'utilisateur.
- Accorder les autorisations de moindre privilège - Lorsque vous définissez des autorisations avec des IAM politiques, accordez uniquement les autorisations nécessaires à l'exécution d'une seule tâche. Pour ce faire, vous définissez les actions qui peuvent être entreprises sur des ressources spécifiques dans des conditions spécifiques, également appelées autorisations de moindre privilège. Pour plus d'informations sur l'utilisation IAM pour appliquer des autorisations, consultez la section Politiques et autorisations IAM dans le guide de IAM l'utilisateur.
- Utiliser des conditions dans IAM les politiques pour restreindre davantage l'accès - Vous pouvez ajouter une condition à vos politiques afin de limiter l'accès aux actions et aux ressources. Par exemple, vous pouvez écrire une condition de stratégie pour spécifier que toutes les demandes doivent être envoyées viaSSL. Vous pouvez également utiliser des conditions pour accorder l'accès aux actions de service si elles sont utilisées via un spécifique Service AWS, comme AWS CloudFormation. Pour plus d'informations, voir Éléments IAM JSON de politique : Condition dans le guide de IAM l'utilisateur.
- Utilisez IAM Access Analyzer pour valider vos IAM politiques afin de garantir des autorisations sécurisées et fonctionnelles : IAM Access Analyzer valide les politiques nouvelles et existantes de manière à ce que les politiques respectent le langage de IAM politique (JSON) et IAM les bonnes pratiques. IAMAccess Analyzer fournit plus de 100 vérifications de politiques et des recommandations exploitables pour vous aider à créer des politiques sécurisées et fonctionnelles.

Pour plus d'informations, consultez la section Validation des politiques d'IAMAccess Analyzer dans le guide de IAM l'utilisateur.

- Authentification multifactorielle (MFA) — Si vous avez un scénario qui nécessite des IAM utilisateurs ou un utilisateur root Compte AWS, activez-la MFA pour plus de sécurité. Pour exiger MFA quand API des opérations sont appelées, ajoutez MFA des conditions à vos politiques. Pour plus d'informations, consultez la section Configuration de l'APIaccès MFA protégé dans le Guide de l'IAMutilisateur.

Pour plus d'informations sur les meilleures pratiques en matière de sécuritéIAM, consultez la section Bonnes pratiques en matière de sécurité IAM dans le Guide de IAM l'utilisateur.

Utilisation de la console sociale de messagerie utilisateur AWS final

Pour accéder à la console sociale AWS End User Messaging, vous devez disposer d'un ensemble minimal d'autorisations. Ces autorisations doivent vous permettre de répertorier et de consulter des informations sur les ressources sociales de messagerie destinées aux utilisateurs AWS finaux dans votre Compte AWS. Si vous créez une politique basée sur l'identité qui est plus restrictive que l'ensemble minimum d'autorisations requis, la console ne fonctionnera pas comme prévu pour les entités (utilisateurs ou rôles) tributaires de cette politique.

Vous n'avez pas besoin d'accorder les autorisations minimales de console pour les utilisateurs qui effectuent des AWS CLI appels uniquement à AWS API. Autorisez plutôt l'accès à uniquement aux actions qui correspondent à l'APIopération qu'ils tentent d'effectuer.

Pour garantir que les utilisateurs et les rôles peuvent toujours utiliser la AWS console de messagerie sociale de l'utilisateur AWS final, associez également la politique sociale *ConsoleAccess* ou *ReadOnly* AWS gérée aux entités. Pour plus d'informations, consultez la section Ajouter des autorisations à un utilisateur dans le Guide de IAM l'utilisateur.

Autorisation accordée aux utilisateurs pour afficher leurs propres autorisations

Cet exemple montre comment créer une stratégie qui permet aux IAM utilisateurs d'afficher les stratégies en ligne et gérées attachées à leur identité d'utilisateur. Cette stratégie inclut les autorisations nécessaires pour réaliser cette action sur la console ou par programmation à l'aide du ou du AWS CLI . AWS API

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

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

AWS politiques gérées pour la messagerie sociale des utilisateurs AWS finaux

Pour ajouter des autorisations à des utilisateurs, des groupes et des rôles, il est plus facile d'utiliser des politiques AWS gérées par que d'écrire des politiques vous-même. Il faut du temps et de l'expertise pour créer des politiques gérées par le IAM client qui ne fournissent aux équipes que les autorisations dont elles ont besoin. Pour démarrer rapidement, vous pouvez utiliser nos stratégies AWS gérées. Ces politiques couvrent des cas d'utilisation courants et sont disponibles dans votre

Compte AWS. Pour plus d'informations sur les politiques AWS gérées, voir les politiques AWS gérées dans le Guide de IAM l'utilisateur.

AWS Les services assurent la maintenance et la mise à jour des politiques AWS gérées. Vous ne pouvez pas modifier les autorisations définies dans les politiques AWS gérées par. Les services ajoutent occasionnellement des autorisations à une politique gérée par AWS pour prendre en charge de nouvelles fonctionnalités. Ce type de mise à jour affecte toutes les identités (utilisateurs, groupes et rôles) auxquelles la politique est attachée. Les services sont très susceptibles de mettre à jour une politique gérée par AWS quand une nouvelle fonctionnalité est lancée ou quand de nouvelles opérations sont disponibles. Les services ne suppriment pas les autorisations d'une politique AWS gérée par, de sorte que les mises à jour de politique n'enfreignent pas vos autorisations existantes.

En outre, AWS prend en charge les stratégies gérées pour les fonctions de tâche qui couvrent plusieurs services. Par exemple, la politique ReadOnlyAccess AWS gérée par donne accès en lecture seule à l'ensemble des AWS services et des ressources. Quand un service lance une nouvelle fonctionnalité, AWS ajoute des autorisations en lecture seule pour les nouvelles opérations et ressources. Pour obtenir la liste et les descriptions des stratégies de fonction de tâche, veuillez consulter les stratégies AWS gérées par pour les fonctions de tâche dans le Guide de IAM l'utilisateur.

AWS Messagerie à l'utilisateur final Mises à jour des politiques AWS gérées sur les réseaux sociaux

Affichez des détails sur les mises à jour des politiques AWS gérées par pour l'utilisateur AWS final Messaging Social depuis que ce service a commencé à suivre ces modifications. Pour obtenir des alertes automatiques concernant les modifications apportées à cette page, abonnez-vous au RSS flux de la page d'historique Document social de l'utilisateur AWS final.

Modification	Description	Date
AWS L'utilisateur final Messaging Social a commencé à suivre les modifications	AWS End User Messaging Social a commencé à suivre les modifications pour ses politiques AWS gérées.	26 septembre 2012 2012 2012 2012 2012 2012 2013

Résolution des problèmes liés AWS à l'identité et à l'accès aux réseaux sociaux des utilisateurs finaux

Utilisez les informations suivantes pour identifier et résoudre les problèmes courants que vous pouvez rencontrer lorsque vous utilisez AWS End User Messaging Social andIAM.

Rubriques

Je ne suis pas autorisé à effectuer une action sur AWS Amazon IVS.

Si vous recevez une erreur qui indique que vous n'êtes pas autorisé à effectuer une action, vos politiques doivent être mises à jour afin de vous permettre d'effectuer l'action.

L'exemple d'erreur suivant se produit lorsque l'`mateojacksonIAM`utilisateur tente d'utiliser la console pour afficher des informations détaillées concernant une *`my-example-widget`* ressource fictive, mais ne dispose pas des `social-messaging:`*`GetWidget`* autorisations fictives nécessaires.

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

Dans ce cas, la politique qui s'applique à l'utilisateur `mateojackson` doit être mise à jour pour autoriser l'accès à la ressource *`my-example-widget`* à l'aide de l'action `social-messaging:`*`GetWidget`*.

Si vous avez encore besoin d'aide, contactez votre AWS administrateur. Votre administrateur vous a fourni vos informations d'identification de connexion.

Je ne suis pas autorisé à effectuer une action dans PassRole

Si vous recevez une erreur selon laquelle vous n'êtes pas autorisé à exécuter l'`iam:PassRole`action, vos stratégies doivent être mises à jour afin de vous permettre de transmettre un rôle à l'utilisateur AWS final Messaging Social.

Certains vous Services AWS permettent de transmettre un rôle existant à ce service au lieu de créer un nouveau rôle de service ou rôle lié à un service. Pour ce faire, un utilisateur doit disposer des autorisations nécessaires pour transmettre le rôle au service.

L'exemple d'erreur suivant se produit lorsqu'un IAM utilisateur nommé `marymajor` essaie d'utiliser la console pour exécuter une action dans AWS End User Messaging Social. Toutefois, l'action nécessite que le service ait des autorisations accordées par un rôle de service. Mary ne dispose pas des autorisations nécessaires pour transférer le rôle au service.

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

Dans ce cas, les politiques de Mary doivent être mises à jour pour lui permettre d'exécuter l'action `iam:PassRole`.

Si vous avez encore besoin d'aide, contactez votre AWS administrateur. Votre administrateur vous a fourni vos informations d'identification de connexion.

Je souhaite permettre à des personnes extérieures Compte AWS à moi d'accéder à mes ressources sociales de messagerie pour les utilisateurs AWS finaux

Vous pouvez créer un rôle que les utilisateurs provenant d'autres comptes ou les personnes extérieures à votre organisation pourront utiliser pour accéder à vos ressources. Vous pouvez spécifier qui est autorisé à assumer le rôle. Pour les services qui prennent en charge les stratégies basées sur les ressources ou les listes de contrôle d'accès (ACLs), vous pouvez utiliser ces stratégies pour accorder aux personnes l'accès à vos ressources.

Pour en savoir plus, consultez les éléments suivants :

- Pour savoir si AWS End User Messaging Social prend en charge ces fonctionnalités, veuillez consulterComment fonctionne AWS Final User Messaging Social IAM.
- Pour savoir comment fournir un accès à vos ressources à des Comptes AWS dont vous êtes propriétaire, veuillez consulter Octroi d'accès à un IAM utilisateur dans un autre Compte AWS que vous possédez dans le Guide de IAM l'utilisateur.
- Pour savoir comment fournir l'accès à vos ressources à des tiers Comptes AWS, veuillez consulter Octroi d'accès à des Comptes AWS appartenant à des tiers dans le Guide de IAM l'utilisateur.
- Pour savoir comment fournir un accès par le biais de la fédération d'identité, veuillez consulter Fournir un accès à des utilisateurs authentifiés en externe (fédération d'identité) dans le Guide de l'IAMutilisateur.

- Pour en savoir plus sur la différence entre l'utilisation des rôles et des politiques basées sur les ressources pour l'accès intercompte, consultez Accès intercompte aux ressources IAM dans le Guide de l'IAMutilisateur.

Validation de conformité pour AWS la messagerie sociale destinée aux utilisateurs finaux

Pour découvrir si un Service AWS fait partie ou non du champ d'application de programmes de conformité spécifiques, veuillez consulter Services AWS dans le champ d'application par programme de de conformité et sélectionnez le programme de conformité qui vous intéresse. Pour des informations générales, voir Programmes de AWS conformité Programmes AWS de .

Vous pouvez télécharger des rapports d'audit externe à l'aide d' AWS Artifact. Pour plus d'https://docs.aws.amazon.com/artifact/latest/ug/downloading-documents.html consultez AWS Artifact.

Votre responsabilité de conformité lors de l'utilisation de vos données Services AWS est déterminée par la sensibilité de vos données, les objectifs de conformité de votre entreprise, ainsi que par la législation et la réglementation applicables. AWS fournit les ressources suivantes pour faciliter la conformité :

- Guides de démarrage rapide de la sécurité et de la conformité : ces guides de déploiement traitent de considérations architecturales et indiquent les étapes à suivre pour déployer des environnements de référence sur AWS qui sont centrés sur la sécurité et la conformité.
- Architecting for HIPAA Security and Compliance on Amazon Web Services : ce livre blanc (en anglais) décrit comment les entreprises peuvent utiliser AWS pour créer HIPAA des applications éligibles.

  > **Note**
  >
  > Tous ne Services AWS sont pas HIPAA éligibles. Pour plus d'informations, consultez le Guide de référence sur les services HIPAA éligibles.

- AWS Ressources de — Cet ensemble de manuels et de guides peut s'appliquer à votre secteur et à votre emplacement..
- AWS Guides de conformité destinés aux clients — Comprenez le modèle de responsabilité partagée sous l'angle de la conformité. Les guides résument les meilleures pratiques pour sécuriser les Services AWS et décrivent les directives relatives aux contrôles de sécurité dans de

nombreux cadres (y compris l'Institut national de normalisation et de technologie (NIST), le Conseil de normes de sécurité (PCI) et l'Organisation internationale de normalisation (ISO)))).

- Évaluation des ressources à l'aide de règles dans le Guide du AWS Config développeur : le AWS Config service évalue dans quelle mesure vos configurations de ressources sont conformes aux pratiques internes, aux directives sectorielles et aux réglementations.
- AWS Security Hub— Cela Service AWS vous propose une vue complète de votre état de sécurité AWS. Security Hub utilise des contrôles de sécurité pour évaluer vos ressources AWS et vérifier votre conformité par rapport aux normes et aux bonnes pratiques du secteur de la sécurité. Pour obtenir la liste des services et des contrôles pris en charge, consultez Référence des contrôles Security Hub.
- Amazon GuardDuty : ce Service AWS détecte les menaces potentielles qui pèsent sur vos Comptes AWS, vos charges de travail, vos conteneurs et vos données en surveillant votre environnement à la recherche d'activités suspectes et malveillantes. GuardDuty peut vous aider à satisfaire diverses exigences de conformité PCIDSS, comme en répondant aux exigences de détection d'intrusion imposées par certains frameworks de conformité.
- AWS Audit Manager: ce service vous Service AWS aide à auditer en continu votre AWS utilisation d'pour simplifier la gestion des risques et la conformité aux réglementations et aux normes du secteur.

Résilience dans AWS la messagerie sociale destinée aux utilisateurs finaux

L'infrastructure AWS mondiale d'repose sur les Régions AWS et les zones de disponibilité. Régions AWS Les fournissent plusieurs zones de disponibilité physiquement séparées et isolées, reliées par un réseau à latence faible, à haut débit et à forte redondance. Avec les zones de disponibilité, vous pouvez concevoir et exploiter des applications et des bases de données qui basculent automatiquement d'une zone à l'autre sans interruption. Les zones de disponibilité sont davantage disponibles, tolérantes aux pannes et ont une plus grande capacité de mise à l'échelle que les infrastructures traditionnelles à un ou plusieurs centres de données.

Pour plus d'informations sur Régions AWS les et les zones de disponibilité, consultez Infrastructure AWS mondiale.

Outre l'infrastructure AWS mondiale, AWS End User Messaging Social propose plusieurs fonctionnalités qui contribuent à la prise en charge des vos besoins en matière de résilience et de sauvegarde de données.

Sécurité de l'infrastructure dans les réseaux sociaux destinés aux utilisateurs AWS finaux

En tant que service géré, AWS End User Messaging Social est protégé par les procédures de sécurité du réseau AWS mondial, qui sont décrites dans le livre blanc Amazon Web Services : Présentation des procédures de sécurité.

Vous utilisez les API appels AWS publiés pour accéder à AWS End User Messaging Social via le réseau. Les clients doivent prendre en charge le protocole TLS (Transport Layer SecurityTLS) 1.0 ou version ultérieure. Nous recommandons TLS TLS 1.2 ou version ultérieure. Les clients doivent également prendre en charge les suites de chiffrement avec une sécurité de transmission parfaite (PFS) comme (Ephemeral Diffie-Hellman) ou DHE ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). La plupart des systèmes modernes tels que Java 7 et les versions ultérieures prennent en charge ces modes.

En outre, les demandes doivent être signées à l'aide d'un ID de clé d'accès et d'une clé d'accès secrète associée à un IAM mandataire. Vous pouvez également utiliser AWS Security Token Service (AWS STS) pour générer des informations d'identification de sécurité temporaires et signer les demandes.

Prévention du cas de figure de l'adjoint désorienté entre services

Le problème de député confus est un problème de sécurité dans lequel une entité qui n'est pas autorisée à effectuer une action peut contraindre une entité plus privilégiée à le faire. Dans AWS, l'emprunt d'identité entre services peut entraîner le problème de député confus. L'usurpation d'identité entre services peut se produire lorsqu'un service (le service appelant) appelle un autre service (le service appelé). Le service appelant peut être manipulé et ses autorisations utilisées pour agir sur les ressources d'un autre client auxquelles on ne serait pas autorisé d'accéder autrement. Pour éviter cela, AWS fournit des outils qui vous aident à protéger vos données pour tous les services avec des principaux de service qui ont eu accès aux ressources de votre compte.

Nous recommandons d'utiliser les clés contextuelles de condition `aws:SourceAccount`globale `aws:SourceArn`et les clés contextuelles dans les politiques de ressources afin de limiter les autorisations que Social Messaging accorde à un autre service à la ressource. Utilisez `aws:SourceArn` si vous souhaitez qu'une seule ressource soit associée à l'accès entre services. Utilisez `aws:SourceAccount` si vous souhaitez autoriser l'association d'une ressource de ce compte à l'utilisation interservices.

Le moyen le plus efficace de se protéger contre le problème de l'adjoint confus consiste à utiliser la clé de contexte de condition `aws:SourceArn` globale avec l'intégralité ARN de la ressource. Si vous ne connaissez pas l'intégralité ARN de la ressource ou si vous spécifiez plusieurs ressources, utilisez la clé de condition de contexte `aws:SourceArn` global avec des caractères génériques (*) pour les parties inconnues de. ARN Par exemple, `arn:aws:social-messaging:*:123456789012:*`.

Si la `aws:SourceArn` valeur ne contient pas l'ID de compte, tel qu'un compartiment Amazon S3ARN, vous devez utiliser les deux clés de contexte de condition globale pour limiter les autorisations.

La valeur de `aws:SourceArn` doit être ResourceDescription.

L'exemple suivant montre comment utiliser les clés de contexte `aws:SourceArn` de condition `aws:SourceAccount` globale dans la messagerie sociale afin d'éviter le problème de l'adjoint confus.

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

Bonnes pratiques de sécurité

AWS End User Messaging Social fournit différentes fonctions de sécurité à prendre en compte lorsque vous développez et implémentez vos propres stratégies de sécurité. Les bonnes pratiques suivantes doivent être considérées comme des instructions générales et ne représentent pas une solution de sécurité complète. Étant donné que ces bonnes pratiques peuvent ne pas être appropriées ou suffisantes pour votre environnement, considérez-les comme des remarques utiles plutôt que comme des recommandations.

- Créez un utilisateur pour chaque personne qui gère les AWS SMS ressources, y compris vous-même. N'utilisez pas d'informations AWS d'identification AWS pour gérer les AWS SMS ressources.
- Accordez à chaque utilisateur un ensemble minimum d'autorisations requises pour exécuter ses tâches.
- Utilisez IAM des groupes IAM pour gérer efficacement des autorisations pour plusieurs utilisateurs.
- Procédez à une rotation régulière des informations d'identification IAM.

Utilisation des rôles liés à un AWS service pour

AWS Final User Messaging Social utilise AWS Identity and Access Management (IAM) des rôles liés au service. Un rôle lié à un service est un type unique de IAM rôle qui est lié directement à AWS End User Messaging Social. Les rôles liés à un service sont prédéfinis par AWS End User Messaging Social et comprennent toutes les autorisations nécessaires au service pour appeler d'autres AWS services en votre nom.

Un rôle lié à un service simplifie AWS la configuration de l'utilisateur final Messaging Social, car vous n'avez pas à ajouter manuellement les autorisations nécessaires. AWS End User Messaging Social définit les autorisations de ses rôles liés à un service et, sauf définition contraire, seul l'utilisateur AWS final Messaging Social peut endosser ses rôles. Les autorisations définies comprennent la stratégie d'approbation et la stratégie d'autorisation. De plus, cette stratégie d'autorisation ne peut pas être attachée à IAM une autre entité.

Vous pouvez supprimer un rôle lié à un service uniquement après la suppression préalable de ses ressources connexes. Vos ressources de messagerie pour les utilisateurs AWS finaux sont ainsi protégées, car vous ne pouvez pas involontairement supprimer l'autorisation d'accéder aux ressources.

Pour plus d'informations sur les autres services qui prennent en charge les rôles liés à un service, consultez AWS Services qui fonctionnent avec IAM et recherchez les services avec un Oui dans la colonne Rôles liés à un service. Choisissez un Oui ayant un lien permettant de consulter les détails du rôle pour ce service.

Autorisations du rôle lié à un service pour Amazon Appelle AWS Scaling

AWS End User Messaging Social utilise le rôle lié au service nommé AWSServiceRoleForSocialMessaging— Pour publier des statistiques et fournir des informations pour l'envoi de vos messages sociaux.

Le rôle AWSServiceRoleForSocialMessaging lié à un service approuve les services suivants pour assumer le rôle :

- `social-messaging.amazonaws.com`

La politique d'autorisations de rôle nommée AWSSocialMessagingServiceRolePolicy permet à l'utilisateur AWS final Messaging Social d'effectuer les actions suivantes sur les ressources spécifiées :

- Action : `"cloudwatch:PutMetricData"` sur `all AWS resources in the AWS/SocialMessaging namespace.`

Vous devez configurer les autorisations de manière à permettre à vos utilisateurs, groupes ou rôles de créer, modifier ou supprimer un rôle lié à un service. Pour plus d'informations, consultez la section Autorisations relatives aux rôles liés à un service dans le Guide de l'IAMutilisateur.

Pour les mises à jour de la politique, voirAWS Messagerie à l'utilisateur final Mises à jour des politiques AWS gérées sur les réseaux sociaux.

Création d'un rôle lié à un service pour AWS Amazon Application Manager

Vous pouvez utiliser la IAM console pour créer un rôle lié à un service avec le cas d'utilisation AWSEndUserMessagingSocial- Metrics. Dans le AWS CLI ou le AWS API, créez un rôle lié au service avec le nom du `social-messaging.amazonaws.com` service. Pour plus d'informations, consultez la section Création d'un rôle lié à un service dans le Guide de l'IAMutilisateur. Si vous supprimez ce rôle lié à un service, vous pouvez utiliser ce même processus pour créer le rôle à nouveau.

Modification d'un rôle lié à un service pour AWS Amazon Application Manager

AWS La messagerie sociale pour l'utilisateur final ne vous permet pas de modifier le rôle AWSServiceRoleForSocialMessaging lié à un service. Une fois que vous avez créé un rôle lié à un service, vous ne pouvez pas changer le nom du rôle, car plusieurs entités peuvent faire référence à ce rôle. Néanmoins, vous pouvez modifier la description du rôle à l'aide deIAM. Pour plus d'informations, consultez la section Modification d'un rôle lié à un service dans le Guide de l'IAMutilisateur.

Suppression d'un rôle lié à un service pour AWS Amazon Application Manager

Si vous n'avez plus besoin d'utiliser une fonctionnalité ou un service qui nécessite un rôle lié à un service, nous vous recommandons de supprimer ce rôle. De cette façon, vous n'avez aucune entité inutilisée qui n'est pas surveillée ou gérée activement. Cependant, vous devez nettoyer les ressources de votre rôle lié à un service avant de pouvoir les supprimer manuellement.

> **Note**
>
> Si le service de messagerie de l'utilisateur AWS final utilise le rôle lorsque vous essayez de supprimer les ressources, la suppression risque d'échouer. Si cela se produit, patientez quelques minutes et réessayez.

Pour supprimer les ressources sociales de messagerie destinées aux utilisateurs AWS finaux utilisées par AWSServiceRoleForSocialMessaging

1. Appelez `list-linked-whatsapp-business-accounts` API pour connaître les ressources dont vous disposez.
2. Pour chaque compte Whats App Business associé, appelez le `disassociate-whatsapp-business-account` API pour retirer la ressource du SocialMessaging service.
3. Vérifiez qu'aucune ressource n'est renvoyée en appelant à `list-linked-whatsapp-business-accounts` API nouveau.

Pour supprimer manuellement le rôle lié à un service à l'aide d'IAM

Utilisez la IAM console AWS CLI, le ou le AWS API pour supprimer le rôle AWSServiceRoleForSocialMessaging lié au service. Pour plus d'informations, consultez la section Suppression d'un rôle lié à un service dans le Guide de l'IAMutilisateur.

Régions prises en charge pour les rôles AWS liés à un service de messagerie électronique de capacité de capacité de capacité de capacité

AWS La messagerie à l'utilisateur final prend en charge l'utilisation des rôles liés à un service dans toutes les régions où le service est disponible. Pour de plus amples informations, veuillez consulter AWS Régions et points de terminaison.

Quotas pour AWS la messagerie sociale destinée aux utilisateurs finaux

Votre AWS compte dispose de quotas par défaut, anciennement appelés limites, pour chaque AWS service. Sauf indication contraire, chaque quota est spécifique à la région. Vous pouvez demander des augmentations pour certains quotas, et d'autres quotas ne peuvent pas être augmentés.

Pour afficher les quotas pour AWS End User Messaging Social ouvrez la console Service Quotas. Dans le volet de navigation, choisissez les AWSservices, puis sélectionnez AWS End User Messaging Social.

Pour demander une augmentation de quota, consultez Demander une augmentation de quota dans le Guide de l'utilisateur de Service Quotas. Si le quota n'est pas encore disponible dans Service Quotas, utilisez le Formulaire d'augmentation de limite de service.

Les quotas de votre AWS compte concernant la messagerie par utilisateur AWS final sur les réseaux sociaux sont les suivants.

Ressource	Par défaut
WhatsApp Compte professionnel (WABA)	25 par région

AWS End User Messaging Social implémente des quotas qui limitent le nombre de demandes que vous pouvez adresser à AWS End User Messaging Social API depuis votre Compte AWS.

Opération	Vitesse
SendWhatsAppMessage	1 000
PostWhatsAppMessageMedia	100
GetWhatsAppMessageMedia	100
DeleteWhatsAppMessageMedia	100
DisassociateWhatsAppBusinessAccount	10

Opération	Vitesse
ListWhatsAppBusinessAccount	10
TagResource	10
UntagResourceRate	10
ListTagsForResourceRate	10

Historique du document pour le Guide de l'utilisateur social de AWS End User Messaging

Le tableau suivant décrit les publications de AWS la documentation pour AWS.

Modification	Description	Date
Première version	Publication initiale du Guide de l'utilisateur social de la messagerie à l'utilisateur AWS final	10 janvier 2024

Les traductions sont fournies par des outils de traduction automatique. En cas de conflit entre le contenu d'une traduction et celui de la version originale en anglais, la version anglaise prévaudra.