Guide de l'utilisateur

AWS Messagerie sociale destinée aux utilisateurs finaux

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

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

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Les marques commerciales et la présentation commerciale d’Amazon ne peuvent pas être utilisées en relation avec un produit ou un service extérieur à Amazon, d’une manière susceptible d’entraîner une confusion chez les clients, ou d’une manière qui dénigre ou discrédite Amazon. Toutes les autres marques commerciales qui ne sont pas la propriété d’Amazon appartiennent à leurs propriétaires respectifs, qui peuvent ou non être affiliés ou connectés à Amazon, ou sponsorisés par Amazon.

Table of Contents

Qu'est-ce que la messagerie sociale destinée aux utilisateurs AWS finaux ? 1
Êtes-vous un utilisateur AWS final de Messaging Social pour la première fois ? 1
Caractéristiques de la messagerie sociale destinée aux utilisateurs AWS finaux 2
Services connexes 2
Accès à AWS la messagerie sociale destinée aux utilisateurs finaux 2
Disponibilité par région 3
Configuration de la messagerie sociale pour les utilisateurs AWS finaux 8
Inscrivez-vous pour un Compte AWS 8
Création d'un utilisateur doté d'un accès administratif 9
Étapes suivantes 10
Premiers pas 11
S'inscrire à WhatsApp 11
Prérequis 11
Inscrivez-vous via la console 13
Étapes suivantes 17
WhatsApp Compte professionnel (WABA) 19
Afficher un WABA 20
Ajouter un WABA 20
WhatsApp types de comptes professionnels 21
Ressources supplémentaires 22
Numéros de téléphone 23
Considérations relatives au numéro de téléphone 23
Ajouter un numéro de téléphone 24
Prérequis 24
Ajouter un numéro de téléphone à un WABA 25
Afficher le statut d'un numéro de téléphone 27
Afficher l'identifiant d'un numéro de téléphone 27
Augmenter les limites des conversations par messagerie 27
Augmenter le débit des messages 29
Comprendre l'évaluation de la qualité des numéros de téléphone 29
Afficher l'évaluation de la qualité d'un numéro de téléphone 30
Modèles de messages 31
Utilisation de modèles de messages avec le WhatsApp gestionnaire 32
Étapes suivantes 32

Rythme des modèles ... 32
Obtenez des commentaires sur le statut réduit d'un modèle ... 33
État du modèle et évaluation de la qualité ... 33
Raisons pour lesquelles un modèle est rejeté ... 35
Destinations des messages et des événements ... 37
Ajouter une destination d'événement ... 37
Prérequis ... 37
Ajouter un message et une destination d'événement ... 38
Règles relatives aux rubriques Amazon SNS chiffrées ... 39
Politiques IAM pour les rubriques Amazon SNS ... 40
Politiques IAM pour Amazon Connect ... 41
Étapes suivantes ... 42
Format du message et de l'événement ... 42
AWS En-tête de l'événement social de messagerie à l'utilisateur final ... 43
Exemple de WhatsApp JSON pour un message ... 44
Exemple de WhatsApp JSON pour un message multimédia ... 45
État du message ... 46
Statuts des messages ... 46
Ressources supplémentaires ... 47
Téléchargement de fichiers multimédia ... 48
Types de fichiers multimédia pris en charge ... 50
Types de fichiers multimédia ... 50
Types de messages ... 53
Ressources supplémentaires ... 53
Envoi de messages ... 54
Envoyer un modèle de message ... 55
Envoi d'un message multimédia ... 56
Répondre à un message reçu ... 59
Modifier le statut d'un message pour qu'il soit lu ... 59
Répondez par une réaction ... 60
Téléchargez un fichier multimédia sur Amazon S3 depuis WhatsApp ... 60
Exemple de réponse à un message ... 61
Prérequis ... 61
Répondant ... 61
Ressources supplémentaires ... 64
Comprendre votre facture ... 65

Facturé par conversation 65
Quand l' FeeType Authentication-International s'applique-t-elle ? 70
Exemple 1 : envoi d'un modèle de message marketing 71
Exemple 2 : ouverture d'une conversation de service 71
Codes ISO de facturation 72
Facturé par message 85
Quand l' FeeType Authentication-International s'applique-t-elle ? 90
Exemple 1 : envoi d'un modèle de message marketing 91
Exemple 2 : ouverture d'une conversation de service 91
Codes ISO de facturation 92
Surveillance 106
Surveillance avec CloudWatch 106
CloudTrail journaux 108
AWS Messagerie à l'utilisateur final Événements liés aux données sociales dans CloudTrail 110
AWS Messagerie à l'utilisateur final Événements de gestion sociale dans CloudTrail 111
AWS Messagerie à l'utilisateur final Exemples d'événements sociaux 112
Bonnes pratiques 114
Up-to-date profil de l'entreprise 114
Obtenir une autorisation 114
Contenu de message interdit 115
Effectuer un audit de vos listes de clients 117
Ajuster votre envoi en fonction de l'implication 117
Envoyer à des heures appropriées 118
Sécurité 119
Protection des données 120
Chiffrement des données 121
Chiffrement en transit 121
Gestion des clés 122
Confidentialité du trafic inter-réseaux 122
Gestion des identités et des accès 123
Public ciblé 123
Authentification par des identités 124
Gestion des accès à l'aide de politiques 128
Comment fonctionne AWS Final User Messaging Social avec IAM 131
Exemples de politiques basées sur l'identité 139

AWS politiques gérées 142
Résolution des problèmes 143
Validation de conformité 145
Résilience 147
Sécurité de l'infrastructure 147
Prévention du cas de figure de l'adjoint désorienté entre services 148
Bonnes pratiques de sécurité 149
Utilisation des rôles liés à un service 150
Autorisations de rôle liées au service pour l'utilisateur AWS final Messaging Social 150
Création d'un rôle lié à un service pour l'utilisateur AWS final Messaging Social 151
Modification d'un rôle lié à un service pour AWS End User Messaging Social 151
Suppression d'un rôle lié à un service pour AWS End User Messaging Social 152
Régions prises en charge pour les AWS rôles liés aux services sociaux de messagerie à l'utilisateur final 152
AWS PrivateLink 153
Considérations 153
Création d'un point de terminaison d'interface 154
Création d'une politique de point de terminaison 154
Quotas 156
Historique de la documentation 157
..... clix

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 fonctionnalités WhatsApp de messagerie de l'entreprise, permettant la création de 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 les SMS et les notifications push. Cela vous permet de communiquer avec les clients par le biais de leur canal de communication préféré.

Pour commencer, créez 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, ou associez un WABA existant au service.

Rubriques

- Êtes-vous un utilisateur AWS final de Messaging Social pour la première fois ?
- Caractéristiques de la messagerie sociale destinée aux utilisateurs AWS finaux
- Services connexes
- Accès à AWS la messagerie sociale destinée aux utilisateurs finaux
- Disponibilité par région

Êtes-vous un utilisateur AWS final de Messaging Social pour 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 des fonctionnalités de messagerie enrichies pour une expérience plus engageante. Au-delà du texte et des médias, vous pouvez envoyer des localisations et des messages interactifs.
- Recevez des SMS et des messages multimédias 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 SMS à l'utilisateur final pour envoyer des SMS
- 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 à Services AWS l'aide de commandes dans l'interpréteur de commandes de votre ligne de commande. AWS Command Line Interface Il est pris 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 commandes de messagerie sociale destinées aux utilisateurs AWS finaux dans la AWS CLI référence des commandes.

AWS SDKs

Si vous préférez créer des applications utilisant des langages spécifiques APIs au lieu de soumettre une demande via HTTP ou HTTPS, utilisez les bibliothèques, les exemples de code, les didacticiels et les autres ressources fournis par. AWS Ces bibliothèques fournissent des fonctions de base qui automatisent les tâches, telles que la signature cryptographique de vos demandes, les nouvelles tentatives et la gestion des réponses aux erreurs. Ces fonctions vous permettent de démarrer plus efficacement. Pour plus d'informations, consultez la section Outils sur lesquels vous pouvez vous appuyer AWS.

Disponibilité par région

AWS La messagerie sociale destinée aux utilisateurs finaux est disponible Régions AWS dans plusieurs pays d'Amérique du Nord, d'Europe, d'Asie et d'Océanie. Dans chaque région, AWS gère 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 élevés de disponibilité et de redondance, tout en minimisant le temps de 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, consultez la section Points de terminaison et quotas pour l'API sociale de messagerie utilisateur AWS final et les points de terminaison de AWS service dans le tableau Référence générale d'Amazon Web Servicesou dans 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 Version de l'API
USA Est (Virginie du Nord)	us-east-1	social-messaging.us-east-1.amazonaws.com social-messaging.us-east-1.api.aws	Version 20 et versions ultérieures

Nom de la région	Région	Point de terminaison	WhatsApp Version de l'API
		social-messaging-fips.us-east-1.amazonaws.com social-messaging-fips.us-east-1.api.aws	
USA Est (Ohio)	us-east-2	social-messaging.us-east-2.amazonaws.com social-messaging.us-east-2.api.aws social-messaging-fips.us-east-2.amazonaws.com social-messaging-fips.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.us-west-2.api.aws social-messaging-fips.us-west-2.amazonaws.com social-messaging-fips.us-west-2.api.aws	Version 20 et versions ultérieures

Nom de la région	Région	Point de terminaison	WhatsApp Version de l'API
Canada (Centre)	ca-central-1	social-messaging.ca-central-1.amazonaws.com social-messaging.ca-central-1.api.aws social-messaging-fips.ca-central-1.amazonaws.com social-messaging-fips.ca-central-1.api.aws	Version 20 et versions ultérieures
Afrique (Le Cap)	af-south-1	social-messaging.af-south-1.amazonaws.com social-messaging.af-south-1.api.aws	Version 20 et versions ultérieures
Asie-Pacifique (Tokyo)	ap-northeast-1	social-messaging.ap-northeast-1.amazonaws.com social-messaging.ap-northeast-1.api.aws	Version 20 et versions ultérieures
Asie-Pacifique (Séoul)	ap-northeast-2	social-messaging.ap-northeast-2.amazonaws.com social-messaging.ap-northeast-2.api.aws	Version 20 et versions ultérieures

Nom de la région	Région	Point de terminaison	WhatsApp Version de l'API
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
Asie-Pacifique (Hyderabad)	ap-south-2	social-messaging.ap-south-2.amazonaws.com social-messaging.ap-south-2.api.aws	Version 20 et versions ultérieures
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
Asie-Pacifique (Sydney)	ap-southeast-2	social-messaging.ap-southeast-2.amazonaws.com social-messaging.ap-southeast-2.api.aws	Version 20 et versions ultérieures
Europe (Francfort)	eu-central-1	social-messaging.eu-central-1.amazonaws.com social-messaging.eu-central-1.api.aws	Version 20 et versions ultérieures

Nom de la région	Région	Point de terminaison	WhatsApp Version de l'API
Europe (Espagne)	eu-south-2	social-messaging.eu-south-2.amazonaws.com social-messaging.eu-south-2.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-2.api.aws	Version 20 et versions ultérieures
Amérique du Sud (São Paulo)	sa-east-1	social-messaging.sa-east-1.amazonaws.com social-messaging.sa-east-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 les étapes suivantes.

Rubriques

- Inscrivez-vous pour un Compte AWS
- Création d'un utilisateur doté d'un accès administratif
- Étapes suivantes

Inscrivez-vous pour un Compte AWS

Si vous n'en avez pas Compte AWS, procédez comme suit pour en créer un.

Pour vous inscrire à un Compte AWS

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

   Une partie de la procédure d'inscription consiste à recevoir un appel téléphonique ou un message texte et à saisir un code de vérification sur le clavier 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 une fois le processus d'inscription terminé. À tout moment, vous pouvez consulter l'activité actuelle de votre compte et gérer votre compte en accédant à https://aws.amazon.com/et en choisissant Mon compte.

Création d’un utilisateur doté d’un accès administratif

Après vous être inscrit à un Compte AWS, sécurisez Utilisateur racine d'un compte AWS 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 en AWS Management Consoletant que propriétaire du compte en choisissant Utilisateur root et en saisissant votre adresse Compte AWS e-mail. 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 racine.

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

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’URL de connexion qui a été envoyée à votre adresse e-mail lorsque vous avez créé l’utilisateur IAM Identity Center.

Pour obtenir de l'aide pour vous connecter en utilisant un utilisateur d'IAM Identity Center, consultez la section Connexion au portail AWS d'accès dans le guide de l'Connexion à AWS 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 travailler avec AWS End User Messaging Social, découvrez comment Commencer à utiliser AWS la messagerie sociale pour les utilisateurs finaux 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 guident dans les étapes à suivre pour associer ou migrer votre compte WhatsApp professionnel (WABA) vers AWS End User Messaging Social.

Rubriques

- S'inscrire à WhatsApp

S'inscrire 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 Un WABA contient les actifs destinés à vos clients, tels que le numéro de téléphone, les modèles et le profil WhatsApp commercial. 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 les réseaux sociaux de messagerie des utilisateurs AWS finaux.

Suivez les étapes décrites dans cette section pour commencer à utiliser AWS End User Messaging Social. Utilisez le processus d'inscription intégré pour créer un nouveau compte WhatsApp professionnel (WABA) ou migrer un WABA existant 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 votre WABA.
- Vous devez nous donner le contrôle de votre WABA. À votre demande, nous vous retransférerons le contrôle de votre WABA 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 une and/or limitations on distribution pursuant to applicable laws and/or réglementation de sauvegarde.
- 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 lors 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 qui peut recevoir un SMS ou un code d'accès à usage unique (OTP) vocal. 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 les SMS, les MMS et les messages vocaux.
- Si vous importez une WABA existante, vous avez besoin de tous PINs les numéros de téléphone associés à la WABA importée. Pour réinitialiser un code PIN perdu ou oublié, suivez les instructions de la section Mise à jour du code PIN dans le guide de référence de l'API WhatsApp Business Platform Cloud.

Les conditions préalables suivantes doivent être remplies pour utiliser une rubrique Amazon SNS ou une instance Amazon Connect comme destination de message et d'événement.

Rubrique Amazon SNS

- Une rubrique Amazon SNS a été créée et des autorisations ont été ajoutées.

> **Note**
>
> Les rubriques FIFO Amazon SNS ne sont pas prises en charge.

- (Facultatif) Pour utiliser une rubrique Amazon SNS chiffrée à l'aide de AWS KMS clés, vous devez accorder à l'utilisateur AWS final des autorisations de messagerie sociale conformément à la politique de clés existante.

Instance Amazon Connect

- Une instance Amazon Connect a été créée et des autorisations ont été ajoutées.

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 WABA existant. 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 professionnel ou la page de profil, entrez l'URL du site Web de votre entreprise ou, si votre entreprise n'a pas de site Web, entrez l'URL de votre page de réseau social.

    d. Dans 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 Nom du compte WhatsApp 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 société 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.
- Dans le champ Description de l'entreprise, entrez une description de votre entreprise. Les clients peuvent consulter la description de votre entreprise dans le cadre de vos coordonnées.
- Dans Site Web, saisissez 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 dans Amazon SNS, 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 Amazon SNS, choisissez soit une nouvelle rubrique standard Amazon SNS et entrez un nom dans le champ Nom de la rubrique, soit choisissez une rubrique standard Amazon SNS existante et choisissez une rubrique dans la liste déroulante des rubriques.

17. Sous Numéros de téléphone :

    Pour chaque numéro de téléphone sous Numéros de WhatsApp téléphone :

    a. Pour vérifier le numéro de téléphone, entrez le code PIN existant ou entrez un nouveau code PIN. Pour réinitialiser un code PIN perdu ou oublié, suivez les instructions de la section Mise à jour du code PIN dans le guide de référence de l'API WhatsApp Business Platform Cloud.

    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 local de l'API Cloud dans le WhatsApp manuel 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 l'enregistrement des événements, y compris l'enregistrement 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.

19. Pour le type de destination, choisissez Amazon SNS ou Amazon Connect

    a. Pour envoyer vos événements vers une destination Amazon SNS, entrez un ARN de rubrique existant dans Topic ARN. Par exemple les stratégies IAM, consultez Politiques IAM pour les rubriques Amazon SNS.

    b. Pour Amazon Connect

        i. Pour l'instance Connect, choisissez une instance dans le menu déroulant.

        ii. Pour Role ARN, choisissez l'une des options suivantes :

            A. Choisissez un rôle IAM existant — Choisissez une politique IAM existante dans le menu déroulant Rôles IAM existants. Par exemple les stratégies IAM, consultez Politiques IAM pour Amazon Connect.

            B. Entrez l'ARN du rôle IAM : entrez l'ARN de la politique IAM dans Utiliser l'ARN du rôle IAM existant. Par exemple les stratégies IAM, consultez Politiques IAM pour Amazon Connect.

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

Étapes suivantes

Une fois votre inscription terminée, 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 SMS 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 les réseaux sociaux de messagerie des utilisateurs AWS finaux

Avec un compte WhatsApp professionnel (WABA), vous pouvez 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. Une WABA ne 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 manuel 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. Elles peuvent être mises 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 votre WABA.
- Vous devez nous accorder le contrôle de votre WABA. À votre demande, nous vous retransférerons le contrôle de votre WABA 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 ou à des restrictions de distribution conformément aux lois 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
- Ajouter un compte WhatsApp professionnel (WABA) dans AWS Final User Messaging Social
- Comprendre les types de comptes WhatsApp professionnels

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

Vous pouvez consulter le WABA associé à votre Compte AWS.

Pour consulter le WABA associé à votre compte

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 un WABA.
3. Dans l'onglet Numéros de téléphone, consultez 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 des 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. Chaque WABA a une limite de 250 modèles.

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

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

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

- Pour ajouter un nouveau 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, puis 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 possède deux types de comptes professionnels :

- 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 tous les utilisateurs. Cette fonctionnalité aide les utilisateurs à identifier les comptes professionnels vérifiés sur WhatsApp.
- Compte professionnel officiel : Outre les avantages d'un compte professionnel, un badge vert apparaît sur le profil et dans les en-têtes des fils de discussion d'un compte professionnel officiel.

  L'approbation d'un compte professionnel WhatsApp officiel (OBA) nécessite de fournir des preuves que l'entreprise est bien connue et reconnue par les consommateurs, telles que des articles, des articles de blog ou des critiques indépendantes. L'approbation d'un WhatsApp OBA n'est 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 souhaitent obtenir un 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 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 de référence de l'API WhatsApp Business Platform Cloud.
- 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
- Ajouter un numéro de téléphone à un compte WhatsApp professionnel (WABA)
- Afficher le statut d'un numéro de téléphone
- Afficher l'identifiant d'un numéro de téléphone dans AWS Final User Messaging Social
- Augmentez les limites de conversation par messagerie dans WhatsApp
- Augmenter le débit des messages dans WhatsApp
- Comprendre l'évaluation de la qualité des numéros de téléphone dans WhatsApp

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 une seule WABA à la fois.
- Le numéro de téléphone peut toujours être utilisé pour les SMS, les MMS et les appels vocaux.
- Chaque numéro de téléphone a reçu une note de qualité de Meta.

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

1. Assurez-vous que le pays ou la région du numéro de téléphone accepte les SMS bidirectionnels.

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 messagerie SMS bidirectionnelle pour le numéro de téléphone. Une fois la configuration terminée, vos SMS entrants sont envoyés à une destination de l'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 pour le numéro de téléphone.

Prérequis

Avant de commencer, les conditions préalables suivantes doivent être remplies :

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

Les conditions préalables suivantes doivent être remplies pour utiliser une rubrique Amazon SNS ou une instance Amazon Connect comme destination de message et d'événement.

Rubrique Amazon SNS

- Une rubrique Amazon SNS a été créée et des autorisations ont été ajoutées.

> **Note**
>
> Les rubriques FIFO Amazon SNS ne sont pas prises en charge.

- (Facultatif) Pour utiliser une rubrique Amazon SNS chiffrée à l'aide de AWS KMS clés, vous devez accorder à l'utilisateur AWS final des autorisations de messagerie sociale conformément à la politique de clés existante.

Instance Amazon Connect

- Une instance Amazon Connect a été créée et des autorisations ont été ajoutées.

Ajouter un numéro de téléphone à un WABA

Pour ajouter un nouveau numéro de téléphone à votre WABA existant

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 WABA et le profil WhatsApp professionnel auxquels vous souhaitez ajouter le 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 WhatsApp téléphone :

    a. Pour vérifier le numéro de téléphone, entrez le code PIN existant ou entrez un nouveau code PIN. Pour réinitialiser un code PIN perdu ou oublié, suivez les instructions de la section Mise à jour du code PIN dans le guide de référence de l'API WhatsApp Business Platform Cloud.

    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 local de l'API Cloud dans le WhatsAppmanuel 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.

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 l'enregistrement des événements, y compris l'enregistrement de la réception d'un message client, activez 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.

13. Pour le type de destination, choisissez Amazon SNS ou Amazon Connect

    a. Pour envoyer vos événements vers une destination Amazon SNS, entrez un ARN de rubrique existant dans Topic ARN. Par exemple les stratégies IAM, consultez Politiques IAM pour les rubriques Amazon SNS.

    b. Pour Amazon Connect

        i. Pour l'instance Connect, choisissez une instance dans le menu déroulant.

        ii. Pour le rôle de canal bidirectionnel, choisissez l'une des options suivantes :

            A. Choisissez un rôle IAM existant — Choisissez une politique IAM existante dans le menu déroulant Rôles IAM existants. Par exemple les stratégies IAM, consultez Politiques IAM pour Amazon Connect.

            B. Entrez l'ARN du rôle IAM : entrez l'ARN de la politique IAM dans Utiliser l'ARN du rôle IAM existant. Par exemple les stratégies IAM, consultez Politiques IAM pour Amazon Connect.

14. 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 initiées par une entreprise 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 MPS de 80. Meta peut augmenter votre MPS à 1 000 si vous répondez aux exigences suivantes :

- Le numéro de téléphone doit être en mesure d'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 sept 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 statut du numéro de téléphone

- Connecté : vous pouvez envoyer des messages dans les limites de votre quota de messages.
- Signalé : La qualité de votre numéro de téléphone est faible et doit être améliorée. Si votre qualité ne s'améliore pas au bout de sept 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. Vous pouvez toujours répondre aux messages entrants. Une fois la période de 24 heures écoulée, 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 un compte WhatsApp professionnel (WABA).
3. Dans l'onglet Numéros de téléphone, consultez votre numéro de téléphone, le nom d'affichage, l'évaluation de la 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

> **Important**
>
> À compter du 01/04/2025, Meta bloquera les modèles de messages marketing envoyés au code de pays américain de. +1 Pour plus d'informations, consultez la section Limites de messages des modèles marketing par utilisateur dans le manuel WhatsAppBusiness Platform Cloud API Reference.

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
- Basé 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 manuel 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 un WABA.
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'examen de Meta peut prendre jusqu'à 24 heures. Meta envoie un e-mail à l'administrateur de votre 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, consultez la section Template pacing dans le manuel 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 un WABA.
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 la 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	Cote de qualité	Signification
En cours de 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

État du modèle	Cote de qualité	Signification
		un faible taux de lecture. Les modèles de message présentant ce statut peuvent être utilisés, mais ils risquent 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 WhatsApp manuel Business Platform Cloud API Reference.

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

Une destination d'événement est une rubrique Amazon SNS ou une instance Amazon Connect vers laquelle les WhatsApp événements sont envoyés. Lorsque vous activez la publication d'événements, tous vos événements d'envoi et de réception sont envoyés à la destination du message et de l'événement. 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
- Format des messages et des événements dans AWS End User Messaging Social
- WhatsApp état du message

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 à la rubrique Amazon SNS. Cela inclut les événements pour chaque numéro de téléphone associé à un compte WhatsApp professionnel. Une rubrique Amazon SNS peut être associée à votre WABA.

Prérequis

Avant de commencer, les conditions préalables suivantes doivent être remplies pour utiliser une rubrique Amazon SNS ou une instance Amazon Connect comme destination de messages et d'événements.

Rubrique Amazon SNS

- Une rubrique Amazon SNS a été créée et des autorisations ont été ajoutées.

> **Note**
>
> Les rubriques FIFO Amazon SNS ne sont pas prises en charge.

- (Facultatif) Pour utiliser une rubrique Amazon SNS chiffrée à l'aide de AWS KMS clés, vous devez accorder à l'utilisateur AWS final des autorisations de messagerie sociale conformément à la politique de clés existante.

Instance Amazon Connect

- Une instance Amazon Connect a été créée et des autorisations ont été ajoutées.

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 un WABA.
3. Dans l'onglet Destination de l'événement, choisissez Modifier la destination.
4. Pour activer une destination d'événement, choisissez Activer.
5. Pour le type de destination, choisissez Amazon SNS ou Amazon Connect

    a. Pour envoyer vos événements vers une destination Amazon SNS, entrez un ARN de rubrique existant dans Topic ARN. Par exemple les stratégies IAM, consultez Politiques IAM pour les rubriques Amazon SNS.

    b. Pour Amazon Connect

        i. Pour l'instance Connect, choisissez une instance dans le menu déroulant.

        ii. Pour le rôle de canal bidirectionnel, choisissez l'une des options suivantes :

            A. Choisissez un rôle IAM existant — Choisissez une politique IAM existante dans le menu déroulant Rôles IAM existants. Par exemple les stratégies IAM, consultez Politiques IAM pour Amazon Connect.

B. Entrez l'ARN du rôle IAM : entrez l'ARN de la politique IAM dans Utiliser l'ARN du rôle IAM existant. Par exemple les stratégies IAM, consultez Politiques IAM pour Amazon Connect.

6. Sélectionnez Enregistrer les modifications.

Règles relatives aux rubriques Amazon SNS chiffrées

Vous pouvez utiliser des rubriques Amazon SNS 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 rubriques Amazon SNS à AWS KMS l'aide de clés, consultez la section Activer la compatibilité entre les sources d'événements AWS issues des services et les rubriques chiffrées dans le manuel Amazon Simple Notification Service Developer Guide.

> **Note**
>
> Les rubriques FIFO Amazon SNS ne sont pas prises en charge.

L'exemple d'instruction utilise les `SourceArn` conditions facultatives mais recommandées pour éviter le problème de confusion des adjoints. Seul le compte propriétaire du réseau social de messagerie de l'utilisateur AWS final y a accès. `SourceAccount` Pour plus d'informations sur le problème des adjoints confus, voir Le problème des adjoints confus dans le guide de l'utilisateur d'IAM.

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

La politique clé doit être modifiée pour permettre à l'utilisateur AWS final 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}:*"
        }
     }
}
```

Politiques IAM pour les rubriques Amazon SNS

Pour utiliser un rôle IAM existant ou pour créer un nouveau rôle, associez la politique suivante à ce rôle afin que AWS End User Messaging Social puisse l'assumer. Pour plus d'informations sur la façon de modifier la relation de confiance d'un rôle, consultez la section Modification d'un rôle dans le guide de l'utilisateur d'IAM.

Voici la politique d'autorisation pour le rôle IAM. La politique d'autorisation autorise la publication sur des rubriques Amazon SNS.

Dans la politique d'autorisation IAM suivante, apportez les modifications suivantes :

- *{PARTITION}*Remplacez-la par la AWS partition dans laquelle vous utilisez AWS End User Messaging Social.
- *{REGION}*Remplacez-le par Région AWS celui dans lequel vous utilisez AWS End User Messaging Social.
- *{ACCOUNT}*Remplacez-le par l'identifiant unique de votre Compte AWS.
- *{TOPIC_NAME}*Remplacez-les par les rubriques Amazon SNS qui recevront des messages.

```
{
    "Effect": "Allow",
    "Principal": {
        "Service": [
          "social-messaging.amazonaws.com"
        ]
```

```
        },
    "Action": "sns:Publish",
    "Resource": "arn:{PARTITION}:sns:{REGION}:{ACCOUNT}:{TOPIC_NAME}"
}
```

Politiques IAM pour Amazon Connect

Si vous souhaitez que AWS End User Messaging Social utilise un rôle IAM existant ou si vous créez un nouveau rôle, associez les politiques suivantes à ce rôle afin que AWS End User Messaging Social puisse l'assumer. Pour plus d'informations sur la façon de modifier une relation de confiance existante d'un rôle, consultez la section Modification d'un rôle dans le guide de l'utilisateur d'IAM. Ce rôle est utilisé à la fois pour envoyer des événements et pour importer des numéros de téléphone depuis AWS End User Messaging Social vers Amazon Connect.

Pour créer de nouvelles politiques IAM, procédez comme suit :

1. Créez une nouvelle politique d'autorisation en suivant les instructions de la section Création de politiques à l'aide de l'éditeur JSON du guide de l'utilisateur IAM.

    - À l'étape 5, utilisez la politique d'autorisation du rôle IAM pour autoriser la publication sur Amazon Connect.

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

```
        }
    ]
}
```

2. Créez une nouvelle politique de confiance en suivant les instructions de la section Création d'un rôle à l'aide de politiques de confiance personnalisées du Guide de l'utilisateur IAM.

   a. À l'étape 4, utilisez la politique de confiance pour le rôle IAM.

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

   b. À l'étape 10, ajoutez la politique d'autorisation que vous avez créée à l'étape précédente.

Étapes suivantes

Une fois que vous avez configuré votre rubrique Amazon SNS, vous devez y abonner un point de terminaison. Le point de terminaison commencera à recevoir les messages publiés sur le sujet associé. Pour plus d'informations sur l'abonnement à une rubrique, consultez la section Abonnement à une rubrique Amazon SNS dans le manuel du développeur Amazon SNS.

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

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

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

L'objet JSON d'un événement contient l'en-tête de l' AWS événement et le code WhatsApp JSON. L'en-tête contient les AWS identifiants ainsi que ceux ARNs de votre compte WhatsApp professionnel (WABA) et de votre numéro de téléphone.

```
{
  "context": {
    "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"
      }
    ]
  },
  "whatsAppWebhookEntry": "{\"...JSON STRING....",
  "aws_account_id": "123456789012",
  "message_timestamp": "2025-01-08T23:30:43.271279391Z",
  "messageId": "6d69f07a-c317-4278-9d5c-6a84078419ec"
}
//Decoding the contents of whatsAppWebhookEntry
{
//WhatsApp notification payload
}
```

Dans l'exemple d'événement précédent :

- *1234567890abcde*est l'identifiant WABA de Meta.
- *abcde1234567890*est l'identifiant du numéro de téléphone de Meta.
- *fb2594b8a7974770b128a409e2example*est l'identifiant du compte WhatsApp professionnel (WABA).
- *976c72a700aac43eaf573ae050example*est l'identifiant du numéro de téléphone.

Exemple de WhatsApp JSON pour recevoir un message

Ce qui suit montre l'enregistrement d'un événement pour un message entrant provenant de WhatsApp. Le JSON reçu WhatsApp dans le `whatsAppWebhookEntry` est reçu sous forme de chaîne JSON et peut être converti en JSON. Pour obtenir la liste des champs et leur signification, consultez la référence de charge utile des notifications Webhooks dans la référence de l'API WhatsApp Business Platform Cloud.

```
{
  "context": {
    "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"
      }
    ]
  },
  "whatsAppWebhookEntry": "{\"...JSON STRING....",
  "aws_account_id": "123456789012",
  "message_timestamp": "2025-01-08T23:30:43.271279391Z",
  "messageId": "6d69f07a-c317-4278-9d5c-6a84078419ec"
}
```

Vous pouvez utiliser un outil, tel que jq, pour convertir la chaîne JSON en JSON. Ce qui suit est `whatsAppWebhookEntry` au format JSON :

```
{
  "id": "503131219501234",
  "changes": [
    {
      "value": {
        "messaging_product": "whatsapp",
        "metadata": {
          "display_phone_number": "14255550123",
```

```
          "phone_number_id": "46271669example"
        },
        "statuses": [
          {
            "id": "wamid.HBgLMTkxNzM5OTI3MzkVAgARGBJBMTM4NDdGRENEREI5Rexample",
            "status": "sent",
            "timestamp": "1736379042",
            "recipient_id": "01234567890",
            "conversation": {
              "id": "62374592e84cb58e52bdaed31example",
              "expiration_timestamp": "1736461020",
              "origin": {
                "type": "utility"
              }
            },
            "pricing": {
              "billable": true,
              "pricing_model": "CBP",
              "category": "utility"
            }
          }
        ]
      },
      "field": "messages"
    }
  ]
}
```

Exemple de WhatsApp JSON pour recevoir un message multimédia

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

```
{
//AWS End User Messaging Social header
}
//Decoding the contents of whatsAppWebhookEntry
{
  "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 état du message

Lorsque vous envoyez un message, vous recevez des mises à jour sur son statut. 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 possibles des messages.

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 bien été envoyé 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 WhatsApp manuel 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 et chargé ou extrait de celui-ci WhatsApp. Le compartiment Amazon S3 doit se trouver dans le même emplacement Compte AWS Région AWS que votre compte WhatsApp professionnel (WABA). Ces instructions indiquent comment créer un compartiment Amazon S3, charger un fichier et créer l'URL du fichier. Pour plus d'informations sur les commandes Amazon S3, consultez Utiliser des commandes de haut niveau (s3) avec l'AWS CLI. Pour plus d'informations sur la configuration du AWS CLI, consultez Configuration de l'interface de ligne de commande AWS dans le guide de AWS Command Line Interface l'utilisateur, création d'un compartiment et téléchargement d'objets dans le guide de l'utilisateur Amazon S3.

> **Note**
>
> WhatsApp stocke les fichiers multimédia pendant 30 jours avant de les supprimer, voir Upload Media in the WhatsApp Business Platform Cloud API Reference.

Vous pouvez également créer une URL présignée vers le fichier multimédia. Avec une URL présignée, 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.

1. Pour créer un compartiment Amazon S3, utilisez la commande create-bucket 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 :

   - *us-east-1*Remplacez-le par Région AWS celui dans lequel se trouve votre WABA.
   - Remplacez *BucketName* par le nom du nouveau compartiment.
2. 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* par le nom à utiliser pour le fichier.

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

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

Pour créer une URL présignée, remplacez-la *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
```

L'URL renvoyée sera : `https://amzn-s3-demo-bucket1.s3.af-south-1.amazonaws.com/mydoc.txt?{Headers}`

3. Téléchargez le fichier multimédia à WhatsApp l'aide de la post-whatsapp-message-mediacommande. Une fois terminée, la commande renvoie le*{MEDIA_ID}*, qui est requis 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 :

- *{ORIGINATION_PHONE_NUMBER_ID}*Remplacez-le par 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

`Content-Type` informations dans le `headers` champ. Si vous utilisez les deux, un `InvalidParameterException` est renvoyé.

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

4. Une fois terminé avec succès, *`MEDIA_ID`* il est renvoyé. Le *`MEDIA_ID`* est utilisé pour référencer le fichier multimédia lors de l'envoi d'un message multimédia.

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 multimédia

Formats audio

Type audio	Extension	Type MIME	Taille maximale
AAC	.aac	audio/aac	16 Mo
AMR	.amr	audio/bras	16 Mo
MP3	.mp3	audio/mpeg	16 Mo
MP4 Audio	.m4a	audio/mp4	16 Mo
Audio OGG	.ogg	audio/ogg	16 Mo

Formats de documents

Types de document	Extension	Type MIME	Taille maximale
Texte	.texte	text/plain	100 Mo

Types de document	Extension	Type MIME	Taille maximale
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	Type MIME	Taille maximale
JPEG	.jpeg	image/jpeg	5 Mo
PNG	.png	image/png	5 Mo

Formats d'autocollants

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

Formats vidéo

Type de vidéo	Extension	Type MIME	Taille maximale
3 GPP	.3 gp	vidéo/3gp	16 Mo
MP4 Vidéo	.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 guide de référence de l'API WhatsApp Business Platform Cloud.

Type de message	Description
Texte	Envoyez un SMS ou une 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	Envoyez un modèle de message.
Emplacement	Envoyez un lieu.
Contacts	Envoyez une carte de visite.
Interactive	Envoyez un message interactif.

Ressources supplémentaires

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

Envoi de messages via WhatsApp AWS Final User Messaging Social

Avant d'envoyer un message, vous devez configurer votre compte WhatsApp professionnel (WABA) et votre utilisateur doit accepter de recevoir des messages de votre part. Pour de plus amples informations, veuillez consulter 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 que lorsqu'une fenêtre de service client est ouverte entre vous et l'utilisateur. Les modèles de messages peuvent être envoyés à tout moment, à condition que l'utilisateur ait choisi 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 `defail`. Vous devez activer un message et une destination d'événement pour recevoir le statut du message.

Pour obtenir la liste des types de messages, consultez la section Messages dans le guide de référence de l'API WhatsApp Business Platform Cloud.

> **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. Elles peuvent être mises 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.

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

Pour plus d'informations sur les types de modèles de messages pouvant être envoyés, consultez la section Modèle de message dans le manuel WhatsApp Business Platform Cloud API Reference. Pour obtenir la liste des types de messages pouvant être envoyés, consultez la section Messages dans le manuel de référence de l'API WhatsApp Business Platform Cloud.

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.

> **Note**
>
> Vous devez spécifier le codage base64 lorsque vous utilisez la AWS CLI version 2. Cela peut être fait en ajoutant le AWS CLI paramètre `--cli-binary-format raw-in-base64-out` ou en modifiant le fichier de configuration AWS CLI global. Pour plus d'informations, consultez le Guide *`cli_binary_format`*de l'utilisateur de l'interface de ligne de AWS commande pour la version 2.

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

Dans la commande précédente, procédez comme suit :

- Remplacez *{PHONE_NUMBER}* par le numéro de téléphone de votre client.
- *{ORIGINATION_PHONE_NUMBER_ID}*Remplacez-le par l'identifiant de votre numéro de téléphone.

L'exemple suivant montre comment envoyer un modèle de message ne contenant aucun composant.

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

- Remplacez *{PHONE_NUMBER}* par le numéro de téléphone de votre client.
- *{ORIGINATION_PHONE_NUMBER_ID}*Remplacez-le par 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 la liste des types de fichiers multimédia pris en charge, consultezTypes et tailles de fichiers multimédia pris en charge dans WhatsApp.

> **Note**
>
> WhatsApp stocke les fichiers multimédia pendant 30 jours avant de les supprimer, voir Upload Media in the WhatsApp Business Platform Cloud API Reference.

1. Téléchargez le fichier multimédia dans un compartiment Amazon S3. Pour de plus amples informations, veuillez consulter Téléchargement de fichiers multimédia à envoyer avec WhatsApp.
2. Téléchargez le fichier multimédia à WhatsApp l'aide de la post-whatsapp-message-mediacommande. En cas de réussite, la commande renverra le*{MEDIA_ID}*, qui est requis 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 :

- *{ORIGINATION_PHONE_NUMBER_ID}*Remplacez-le par 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 `Content-Type` informations dans le `headers` champ. 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
```

> **Note**
>
> Vous devez spécifier le codage base64 lorsque vous utilisez la AWS CLI version 2. Cela peut être fait en ajoutant le AWS CLI paramètre `--cli-binary-format raw-in-base64-out` ou en modifiant le fichier de configuration AWS CLI global. Pour plus d'informations, consultez le Guide *cli_binary_format*de l'utilisateur de l'interface de ligne de AWS commande pour la version 2.
>
> ```
> aws socialmessaging send-whatsapp-message --message
>  '{"messaging_product":"whatsapp","to":"'{PHONE_NUMBER}'","type":"image","image":
> {"id":"'{MEDIA_ID}'"}}' --origination-phone-number-
> id {ORIGINATION_PHONE_NUMBER_ID} --meta-api-version v20.0 --cli-binary-
> format raw-in-base64-out
> ```

Dans la commande précédente, procédez comme suit :

- Remplacez *{PHONE_NUMBER}* par le numéro de téléphone de votre client.
- *{ORIGINATION_PHONE_NUMBER_ID}*Remplacez-le par l'identifiant de votre numéro de téléphone.
- Remplacez *{MEDIA_ID}* par l'identifiant 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 :

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

Répondre à un message dans AWS End User Messaging Social

Avant de pouvoir recevoir un SMS ou un message multimédia, vous devez avoir configuré votre compte WhatsApp professionnel (WABA) et une destination pour l'événement. Lorsque vous recevez un message entrant, un événement est enregistré dans la rubrique Amazon SNS de destination de l'événement. Pour recevoir une notification, vous devez vous abonner au point de terminaison des rubriques Amazon SNS.

Pour un exemple d'événement lié à la réception d'un message multimédia, voirExemple de WhatsApp JSON pour recevoir 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 obtenir la liste des types de fichiers multimédia pris en charge, consultezTypes et tailles de fichiers multimédia pris en charge dans WhatsApp.

> **Important**
>
> Pour recevoir des messages entrants, vous devez activer les destinations d'événements pour la WABA. Pour de plus amples informations, veuillez consulter Ajouter 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 dans 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 :

- *{ORIGINATION_PHONE_NUMBER_ID}*Remplacez-le par 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 de la rubrique Amazon SNS.

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 le numéro de téléphone de votre client.
- Remplacez *{MESSAGE_ID}* par l'identifiant unique du message. Utilisez la valeur du `id` champ dans l'objet du message de la rubrique Amazon SNS.
- *{ORIGINATION_PHONE_NUMBER_ID}*Remplacez-le par 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}* par la valeur du `id` champ de l'événement reçu. Pour un exemple d'événement multimédia entrant, voirExemple de WhatsApp JSON pour recevoir un message multimédia.
- *{ORIGINATION_PHONE_NUMBER_ID}*Remplacez-le par 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 avec accusé de lecture et 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

Pour recevoir une notification indiquant que Diego a envoyé un message, vous devez avoir configuré une rubrique Amazon SNS destinée à l'événement et vous être abonné à un point de terminaison de rubrique.

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 lancé la conversation, cela n'est pas pris en compte dans le quota de conversations initiées par votre entreprise.

`whatsAppWebhookEntry`Dans cet exemple, il est présenté en notation JSON. Pour un exemple de conversion de la `whatsAppWebhookEntry` chaîne from JSON en JSON, consultezExemple de WhatsApp JSON pour recevoir un message.

```
{
  "context": {
    "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"
      }
    ]
  },
  "whatsAppWebhookEntry": "{\"...JSON STRING....",
  "aws_account_id": "123456789012",
  "message_timestamp": "2025-01-08T23:30:43.271279391Z"
}
//Decoding the contents of whatsAppWebhookEntry
{
  "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.

> **Note**
>
> Vous devez spécifier le codage base64 lorsque vous utilisez la AWS CLI version 2. Cela peut être fait en ajoutant le AWS CLI paramètre `--cli-binary-format raw-in-base64-out` ou en modifiant le fichier de configuration AWS CLI global. Pour plus d'informations, consultez le Guide *cli_binary_format*de l'utilisateur de l'interface de ligne de AWS commande pour la version 2.

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

Dans la commande précédente, procédez comme suit :

- Remplacez *{ORIGINATION_PHONE_NUMBER_ID}* par le numéro de téléphone auquel Diego a envoyé son messagephone-number-id-976c72a700aac43eaf573ae050example.
- Remplacez *{MESSAGE_ID}* par l'identifiant unique du message. Il s'agit de la même valeur que celle du `id` champ dans le message reçuwamid.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 :

- Remplacer *{PHONE_NUMBER}* par le numéro de téléphone de Diego,14255550150.
- Remplacez *{MESSAGE_ID}* par l'identifiant unique du message. Il s'agit de la même valeur que celle du `id` champ dans le message reçuwamid.HBgLMTQyNTY5ODgzMDIVAgASGCBDNzBDRjM5MDU2ODEwMDkwREY4ODBDRDE0RjVGRk
- Remplacez *{ORIGINATION_PHONE_NUMBER_ID}* par 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 manuel de référence de l'API WhatsApp Business Platform Cloud.

Comprendre les rapports WhatsApp de facturation et d'utilisation pour AWS Final User Messaging Social

Il existe deux types de rapports de WhatsApp facturation et d'utilisation pour AWS End User Messaging Social :

- Facturé par conversation
- Facturé par message

Pour plus d'informations sur ces types de facturation et de rapport, consultez les rubriques suivantes.

Rubriques

- Facturé par conversation
- Facturé par message

Facturé par conversation

> **Note**
>
> À compter du 1er juillet 2025, AWS End User Messaging Social facturera par message plutôt que par conversation pour les WhatsApp messages, conformément à la modification de Meta. Cela signifie que vous êtes facturé un méta-frais au `MetaTemplateMessageFee` lieu du AWS `MessageFee`. `ConversationFee` Ces modifications sont incluses dans vos factures mensuelles, à compter de la facture de juillet 2025 que vous recevez en août 2025. Pour plus d'informations sur la facturation et les rapports d'utilisation lorsque vous êtes facturé par message, consultezthe section called "Facturé par message".

Le canal social de messagerie à l'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

au cours de laquelle 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, voir WhatsAppla section Tarification des messages destinés aux utilisateurs AWS finaux.

Champ	Options	Description
`Region code`	• USE1— Région de l'Est des États-Unis (Virginie du Nord) • USE2— Région de l'est des États-Unis (Ohio) • USW2— Région ouest des États-Unis (Oregon) • APS3— Région Asie-Paci fique (Mumbai) • APS5— Région Asie-Paci fique (Hyderabad) • APS1— Région Asie-Paci fique (Singapour) • APS2— Région Asie-Paci fique (Sydney) • EU : région Europe (Irlande) • EUW2— Région Europe (Londres) • APN1— Région Asie-Paci fique (Tokyo) • APN2— Région Asie-Paci fique (Séoul)	Le Région AWS préfixe qui indique l'endroit d'où le WhatsApp message a été envoyé ou reçu.

Champ	Options	Description
	• EUC1— Région Europe (Francfort) • EUS2— Région Europe (Espagne) • SAE1— Région Amérique du Sud (São Paulo) • AFS1— Région Afrique (Cape Town) • CAN1— Région du Canada (Centre)	
MessagingType	`WhatsApp`	Ce champ identifie le type de message envoyé.
ISO	Voir les pays pris en charge	Code de pays ISO 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` , `Authentication-International` , `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 de l'inscription, order/delivery la gestion (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). • `Authentication-International` — Utilisé de la même manière que`Authentication` , mais votre entreprise est éligible aux tarifs Authentication-International, basés dans un autre pays, et la conversation a été ouverte à l'heure de début du pays ou après cette date. • `Service`— Utilisé pour résoudre les demandes des clients. **`ConversationFee`** Catégories créées par l'utilisateur • `Service`— Utilisé pour résoudre les demandes des clients.

Champ	Options	Description
		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
```

Quand l' FeeType Authentication-International s'applique-t-elle ?

Pour obtenir la liste des pays dotés d'un `Authentication-International` FeeType, voir WhatsAppla section Tarification des messages destinés aux utilisateurs AWS finaux.

Si vous ouvrez une `Authentication` conversation avec un WhatsApp utilisateur dont le code d'appel du pays comporte un `Authentication-International` FeeType, le `Authentication-International` tarif de ce pays vous sera facturé si :

1. Votre entreprise ouvre plus de 750 000 conversations sur une période mobile de 30 jours sur l'ensemble de vos comptes WhatsApp professionnels avec des WhatsApp utilisateurs dont le code

d'appel correspond à un pays qui applique un `Authentication-International` tarif. Pour plus d'informations, consultez la section Eligibilité dans le guide du développeur de WhatsApp Business Platform.

> **Important**
>
> Si Meta détermine que votre entreprise est éligible`Authentication-International`, elle tentera de vous envoyer une notification par e-mail indiquant les pays concernés et les heures de début reportées sur une période de 30 jours.

2. Votre entreprise est basée dans un autre pays. Pour plus d'informations sur la gestion de l'emplacement de votre entreprise, consultez la section Emplacement commercial principal dans le Guide du développeur de WhatsApp Business Platform.
3. La conversation a été ouverte le jour ou après votre heure de départ dans ce pays

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, codes ISO de facturation sociale et cartographie des frais de WhatsApp conversation

Pays pris en charge

Code de pays ISO à deux chiffres	Nom du pays	WhatsApp région de facturation des conversations
AF	Afghanistan	Rest of Asia Pacific
AX	Aland Islands	Other
AL	Albania	Rest of Central & Eastern Europe
DZ	Algeria	Rest of Africa
AS	American Samoa	Other
AD	Andorra	Other
AO	Angola	Rest of Africa
AI	Anguilla	Other
AQ	Antarctica	Other
AG	Antigua and Barbuda	Other
AR	Argentina	Argentina
AM	Armenia	Rest of Central & Eastern Europe
AW	Aruba	Other
AC	Ascension Island	Other
AU	Australia	Rest of Asia Pacific
AT	Austria	Rest of Western Europe

Code de pays ISO à deux chiffres	Nom du pays	WhatsApp région de facturation des conversations
AZ	Azerbaijan	Rest of Central & Eastern Europe
BS	Bahamas	Other
BH	Bahrain	Rest of Middle East
BD	Bangladesh	Rest of Asia Pacific
BB	Barbados	Other
BY	Belarus	Rest of Central & Eastern Europe
BE	Belgium	Rest of Western Europe
BZ	Belize	Other
BJ	Benin	Rest of Africa
BM	Bermuda	Other
BT	Bhutan	Other
BO	Bolivia	Rest of Latin America
BQ	Bonaire	Other
BA	Bosnia and Herzegovina	Other
BW	Botswana	Rest of Africa
BV	Bouvet Island	Other
BR	Brazil	Brazil
IO	British Indian Ocean Territory	Other
VG	British Virgin Islands	Other

Code de pays ISO à deux chiffres	Nom du pays	WhatsApp région de facturation des conversations
BN	Brunei Darussalam	Other
BG	Bulgaria	Rest of Central & Eastern Europe
BF	BurkinaFaso	Rest of Africa
BI	Burundi	Rest of Africa
KH	Cambodia	Rest of Asia Pacific
CM	Cameroon	Rest of Africa
CA	Canada	North America
CV	Cape Verde	Other
KY	Cayman Islands	Other
CF	Central African Republic	Other
TD	Chad	Rest of Africa
CL	Chile	Chile
CN	China	Rest of Asia Pacific
CX	Christmas Island	Other
CC	Cocos(Keeling) Islands	Other
CO	Colombia	Colombia
KM	Comoros	Other
CK	Cook Islands	Other
CR	Costa Rica	Rest of Latin America

Code de pays ISO à deux chiffres	Nom du pays	WhatsApp région de facturation des conversations
CI	Cote d'Ivoire	Rest of Africa
HR	Croatia	Rest of Central & Eastern Europe
CW	Curacao	Other
CY	Cyprus	Other
CZ	Czech Republic	Rest of Central & Eastern Europe
CD	Democratic Republic of the Congo	Rest of Africa
DK	Denmark	Rest of Western Europe
DJ	Djibouti	Other
DM	Dominica	Other
DO	Dominican Republic	Rest of Latin America
EC	Ecuador	Rest of Latin America
EG	Egypt	Egypt
SV	El Salvador	Rest of Latin America
GQ	Equatorial Guinea	Other
ER	Eritrea	Rest of Africa
EE	Estonia	Other
ET	Ethiopia	Rest of Africa
SZ	Eswatini	Rest of Africa

Code de pays ISO à deux chiffres	Nom du pays	WhatsApp région de facturation des conversations
FK	Falkland Islands	Other
FO	Faroe Islands	Other
FJ	Fiji	Other
FI	Finland	Rest of Western Europe
FR	France	France
GF	French Guiana	Other
PF	French Polynesia	Other
TF	French Southern Territories	Other
GA	Gabon	Rest of Africa
GM	Gambia	Rest of Africa
GE	Georgia	Rest of Central & Eastern Europe
DE	Germany	Germany
GH	Ghana	Rest of Africa
GI	Gibraltar	Other
GR	Greece	Rest of Central & Eastern Europe
GL	Greenland	Other
GD	Grenada	Other
GP	Guadeloupe	Other
GU	Guam	Other

Code de pays ISO à deux chiffres	Nom du pays	WhatsApp région de facturation des conversations
GT	Guatemala	Rest of Latin America
GG	Guernsey	Other
GN	Guinea	Other
GW	Guinea-Bissau	Rest of Africa
GY	Guyana	Other
HT	Haiti	Rest of Latin America
HM	Heard and McDonald Islands	Other
HN	Honduras	Rest of Latin America
HK	Hong Kong	Rest of Asia Pacific
HU	Hungary	Rest of Central & Eastern Europe
IS	Iceland	Other
IN	India	India
ID	Indonesia	Indonesia
IQ	Iraq	Rest of Middle East
IE	Ireland	Rest of Western Europe
IM	Isle of Man	Other
IL	Israel	Israel
IT	Italy	Italy
JM	Jamaica	Rest of Latin America

Code de pays ISO à deux chiffres	Nom du pays	WhatsApp région de facturation des conversations
JP	Japan	Rest of Asia Pacific
JE	Jersey	Other
JO	Jordan	Rest of Middle East
KZ	Kazakhstan	Other
KE	Kenya	Rest of Africa
KI	Kiribati	Other
XK	Kosovo	Other
KW	Kuwait	Rest of Middle East
KG	Kyrgyzstan	Other
LA	Lao PDR	Rest of Asia Pacific
LV	Latvia	Rest of Central & Eastern Europe
LB	Lebanon	Rest of Middle East
LS	Lesotho	Rest of Africa
LR	Liberia	Rest of Africa
LY	Libya	Rest of Africa
LI	Liechtenstein	Other
LT	Lithuania	Rest of Central & Eastern Europe
LU	Luxembourg	Other
MO	Macao	Other

Code de pays ISO à deux chiffres	Nom du pays	WhatsApp région de facturation des conversations
MK	Macedonia	Rest of Central & Eastern Europe
MG	Madagascar	Rest of Africa
MW	Malawi	Rest of Africa
MY	Malaysia	Malaysia
MV	Maldives	Other
ML	Mali	Rest of Africa
MT	Malta	Other
MH	Marshall Islands	Other
MQ	Martinique	Other
MR	Mauritania	Rest of Africa
MU	Mauritius	Other
YT	Mayotte	Other
MX	Mexico	Mexico
FM	Micronesia	Other
MD	Moldova	Rest of Central & Eastern Europe
MC	Monaco	Other
MN	Mongolia	Rest of Asia Pacific
ME	Montenegro	Other
MS	Montserrat	Other

Code de pays ISO à deux chiffres	Nom du pays	WhatsApp région de facturation des conversations
MA	Morocco	Rest of Africa
MZ	Mozambique	Rest of Africa
MM	Myanmar	Other
NA	Namibia	Rest of Africa
NR	Nauru	Other
NP	Nepal	Rest of Asia Pacific
NL	Netherlands	Netherlands
NC	New Caledonia	Other
NZ	New Zealand	Rest of Asia Pacific
NI	Nicaragua	Rest of Latin America
NE	Niger	Rest of Africa
NG	Nigeria	Nigeria
NU	Niue	Other
NF	Norfolk Island	Other
MP	Northern Mariana Islands	Other
NO	Norway	Rest of Western Europe
OM	Oman	Rest of Middle East
PK	Pakistan	Pakistan
PW	Palau	Other
PS	Palestinian Territory	Other

Code de pays ISO à deux chiffres	Nom du pays	WhatsApp région de facturation des conversations
PA	Panama	Rest of Latin America
PG	Papua New Guinea	Rest of Asia Pacific
PY	Paraguay	Rest of Latin America
PE	Peru	Peru
PH	Philippines	Rest of Asia Pacific
PN	Pitcairn	Other
PL	Poland	Rest of Central & Eastern Europe
PT	Portugal	Rest of Western Europe
PR	Puerto Rico	Rest of Latin America
QA	Qatar	Rest of Middle East
CG	Republic of Congo	Other
RE	Reunion	Other
RO	Romania	Rest of Central & Eastern Europe
RU	Russian Federation	Russia
RW	Rwanda	Rest of Africa
SH	Saint Helena	Other
KN	Saint Kitts and Nevis	Other
LC	Saint Lucia	Other
PM	Saint Pierre and Miquelon	Other

Code de pays ISO à deux chiffres	Nom du pays	WhatsApp région de facturation des conversations
VC	Saint Vincent and Grenadines	Other
BL	Saint-Barthelemy	Other
MF	Saint-Martin	Other
WS	Samoa	Other
SM	San Marino	Other
ST	Sao Tome and Principe	Other
SA	Saudi Arabia	Saudi Arabia
SN	Senegal	Rest of Africa
RS	Serbia	Rest of Central & Eastern Europe
SC	Seychelles	Other
SL	Sierra Leone	Rest of Africa
SG	Singapore	Rest of Asia Pacific
SX	Sint Maarten	Other
SK	Slovakia	Rest of Central & Eastern Europe
SI	Slovenia	Rest of Central & Eastern Europe
SB	Solomon Islands	Other
SO	Somalia	Rest of Africa
ZA	South Africa	South Africa

Code de pays ISO à deux chiffres	Nom du pays	WhatsApp région de facturation des conversations
GS	South Georgia and the South Sandwich Islands	Other
KR	South Korea	Other
SS	South Sudan	Rest of Africa
ES	Spain	Spain
LK	Sri Lanka	Rest of Asia Pacific
SR	Suriname	Other
SJ	Svalbard and Jan Mayen Islands	Other
SE	Sweden	Rest of Western Europe
CH	Switzerland	Rest of Western Europe
TW	Taiwan	Rest of Asia Pacific
TJ	Tajikistan	Rest of Asia Pacific
TZ	Tanzania	Rest of Africa
TH	Thailand	Rest of Asia Pacific
TL	Timor-Leste	Other
TG	Togo	Rest of Africa
TK	Tokelau	Other
TO	Tonga	Other
TT	Trinidad and Tobago	Other
TA	Tristan da Cunha	Other

Code de pays ISO à deux chiffres	Nom du pays	WhatsApp région de facturation des conversations
TN	Tunisia	Rest of Africa
TR	Turkey	Turkey
TM	Turkmenistan	Rest of Asia Pacific
TC	Turks and Caicos Islands	Other
TV	Tuvalu	Other
UG	Uganda	Rest of Africa
UA	Ukraine	Rest of Central & Eastern Europe
AE	United Arab Emirates	United Arab Emirates
GB	United Kingdom	United Kingdom
US	United States	North America
UY	Uruguay	Rest of Latin America
UM	US Minor Outlying Islands	Other
UZ	Uzbekistan	Rest of Asia Pacific
VU	Vanuatu	Other
VA	Vatican City State	Other
VE	Venezuela	Rest of Latin America
VN	Vietnam	Rest of Asia Pacific
VI	Virgin Islands	Other
WF	Wallis and Futuna Islands	Other

Code de pays ISO à deux chiffres	Nom du pays	WhatsApp région de facturation des conversations
EH	Western Sahara	Other
YE	Yemen	Rest of Middle East
ZM	Zambia	Rest of Africa
ZW	Zimbabwe	Other

Facturé par message

> **Note**
>
> À compter du 1er juillet 2025, AWS End User Messaging Social facturera par message plutôt que par conversation pour les WhatsApp messages, conformément à la modification de Meta. Cela signifie que vous êtes facturé un méta-frais au `MetaTemplateMessageFee` lieu du AWS `MessageFee`. `ConversationFee` Ces modifications sont incluses dans vos factures mensuelles, à compter de la facture de juillet 2025 que vous recevez en août 2025. Pour comprendre les factures antérieures sur la base de`ConversationFee`, voirthe section called "Facturé par conversation".

Le canal social de messagerie à l'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 message : le`MetaTemplateMessageFee`, et le AWS `MessageFee`.

Lorsque vous envoyez un modèle de message, vous êtes facturé un WhatsApp `MetaTemplateMessageFee` et un AWS par. `MessageFee`

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, voir WhatsAppla section Tarification des messages destinés aux utilisateurs AWS finaux.

Champ	Options	Description
Region code	• USE1— Région de l'Est des États-Unis (Virginie du Nord) • USE2— Région de l'est des États-Unis (Ohio) • USW2— Région ouest des États-Unis (Oregon) • APS3— Région Asie-Pacifique (Mumbai) • APS5— Région Asie-Pacifique (Hyderabad) • APS1— Région Asie-Pacifique (Singapour) • APS2— Région Asie-Pacifique (Sydney) • EU : région Europe (Irlande) • EUW2— Région Europe (Londres) • APN1— Région Asie-Pacifique (Tokyo) • APN2— Région Asie-Pacifique (Séoul) • EUC1— Région Europe (Francfort) • EUS2— Région Europe (Espagne) • SAE1— Région Amérique du Sud (São Paulo) • AFS1— Région Afrique (Cape Town) • CAN1— Région du Canada (Centre)	Le Région AWS préfixe qui indique l'endroit d'où le WhatsApp message a été envoyé ou reçu.

Champ	Options	Description
MessagingType	WhatsApp	Ce champ identifie le type de message envoyé.
ISO	Voir les pays pris en charge	Code de pays ISO à deux chiffres auquel le message a été envoyé.
FeeDescription	MetaTemplateMessageFee , MessageFee	Ce champ spécifie soit le, WhatsApp MetaTemplateMessageFee soit le AWS perMessageFee .

Champ	Options	Description
FeeType	`Authentication` , `Authentication-International` , `Marketing` , `Service`, `Utility`, `Standard`	Ce champ affiche le type de message utilisé ou indique la norme pour les frais par message **`MetaTemplateMessageFee`** 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 de l'inscription, order/delivery la gestion (par exemple une mise à jour de livraison), les mises à jour du compte ou les alertes (par exemple un rappel de paiement)

Champ	Options	Description
		ou les enquêtes de feedback. • `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). • `Authentication-International` — Utilisé de la même manière que`Authentication` , mais votre entreprise est éligible aux tarifs Authentication-International, basés dans un autre pays, et le message a été envoyé à l'heure de début du voyage dans le pays ou après cette date. • `Service`— Utilisé pour résoudre les demandes des clients.

Champ	Options	Description
		`MetaTemplateMessageFee` 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 envoyez un modèle de message, vous êtes facturé pour un `MetaTemplateMessageFee` et un`MessageFee`. Lorsque vous envoyez des SMS en format libre ou que vous recevez des messages entrants, le. `MessageFee`

Par exemple, si vous envoyez un modèle de message marketing à un client, le `MetaTemplateMessageFee` et `MessageFee` vous sont facturés.

Quand l' FeeType Authentication-International s'applique-t-elle ?

Pour obtenir la liste des pays dotés d'un `Authentication-International` FeeType, voir WhatsAppla section Tarification des messages destinés aux utilisateurs AWS finaux.

Si vous envoyez un `Authentication` message à un WhatsApp utilisateur dont le code d'appel du pays comporte un `Authentication-International` FeeType, le `Authentication-International` tarif de ce pays vous sera facturé si :

1. Votre entreprise ouvre plus de 750 000 messages sur une période mobile de 30 jours sur l'ensemble de vos comptes WhatsApp professionnels auprès d' WhatsApp utilisateurs dont le code d'appel correspond à un pays où le tarif est appliqué. `Authentication-International` Pour plus d'informations, consultez la section Eligibilité dans le guide du développeur de WhatsApp Business Platform.

> **Important**
>
> Si Meta détermine que votre entreprise est éligible`Authentication-International`, elle tentera de vous envoyer une notification par e-mail indiquant les pays concernés et les heures de début reportées sur une période de 30 jours.

2. Votre entreprise est basée dans un autre pays. Pour plus d'informations sur la gestion de l'emplacement de votre entreprise, consultez la section Emplacement commercial principal dans le Guide du développeur de WhatsApp Business Platform.
3. Le message a été envoyé à l'heure de début de la période de 30 jours pour ce pays ou après cette date.

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 `MetaTemplateMessageFee` et un AWS par. `MessageFee`

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

Exemple 2 : ouverture d'une conversation de service

Une conversation de service est créée lorsqu'une entreprise répond au message entrant d'un utilisateur dans les 24 heures suivant la réception du message initié par l'utilisateur. Dans ce scénario, vous êtes facturé un `MetaTemplateMessageFee-Service_Regular` frais et un AWS `MessageFee` pour chaque message entrant et sortant. Par exemple, si un utilisateur a envoyé un message, que l'entreprise a répondu et que l'utilisateur a répondu, les frais pour les trois messages seraient les suivants :

```
User Initiated Message 1: APS1-WhatsApp-CA-MessageFee-StandardService
Business Initiated Message 2: APS1-WhatsApp-CA-MetaTemplateMessageFee-Service_Regular
Business Initiated Message 2: APS1-WhatsApp-CA-MessageFee-StandardService
User Initiated Message 3: APS1-WhatsApp-CA-MessageFee-StandardService
```

AWS Messagerie à l'utilisateur final, codes ISO de facturation sociale et MetaTemplateMessageFee cartographie

Pays pris en charge

Code de pays ISO à deux chiffres	Nom du pays	WhatsApp région de facturation des conversations
AF	Afghanistan	Rest of Asia Pacific
AX	Aland Islands	Other
AL	Albania	Rest of Central & Eastern Europe
DZ	Algeria	Rest of Africa
AS	American Samoa	Other
AD	Andorra	Other
AO	Angola	Rest of Africa
AI	Anguilla	Other
AQ	Antarctica	Other
AG	Antigua and Barbuda	Other
AR	Argentina	Argentina
AM	Armenia	Rest of Central & Eastern Europe
AW	Aruba	Other
AC	Ascension Island	Other
AU	Australia	Rest of Asia Pacific
AT	Austria	Rest of Western Europe

Code de pays ISO à deux chiffres	Nom du pays	WhatsApp région de facturation des conversations
AZ	Azerbaijan	Rest of Central & Eastern Europe
BS	Bahamas	Other
BH	Bahrain	Rest of Middle East
BD	Bangladesh	Rest of Asia Pacific
BB	Barbados	Other
BY	Belarus	Rest of Central & Eastern Europe
BE	Belgium	Rest of Western Europe
BZ	Belize	Other
BJ	Benin	Rest of Africa
BM	Bermuda	Other
BT	Bhutan	Other
BO	Bolivia	Rest of Latin America
BQ	Bonaire	Other
BA	Bosnia and Herzegovina	Other
BW	Botswana	Rest of Africa
BV	Bouvet Island	Other
BR	Brazil	Brazil
IO	British Indian Ocean Territory	Other
VG	British Virgin Islands	Other

Code de pays ISO à deux chiffres	Nom du pays	WhatsApp région de facturation des conversations
BN	Brunei Darussalam	Other
BG	Bulgaria	Rest of Central & Eastern Europe
BF	BurkinaFaso	Rest of Africa
BI	Burundi	Rest of Africa
KH	Cambodia	Rest of Asia Pacific
CM	Cameroon	Rest of Africa
CA	Canada	North America
CV	Cape Verde	Other
KY	Cayman Islands	Other
CF	Central African Republic	Other
TD	Chad	Rest of Africa
CL	Chile	Chile
CN	China	Rest of Asia Pacific
CX	Christmas Island	Other
CC	Cocos(Keeling) Islands	Other
CO	Colombia	Colombia
KM	Comoros	Other
CK	Cook Islands	Other
CR	Costa Rica	Rest of Latin America

Code de pays ISO à deux chiffres	Nom du pays	WhatsApp région de facturation des conversations
CI	Cote d'Ivoire	Rest of Africa
HR	Croatia	Rest of Central & Eastern Europe
CW	Curacao	Other
CY	Cyprus	Other
CZ	Czech Republic	Rest of Central & Eastern Europe
CD	Democratic Republic of the Congo	Rest of Africa
DK	Denmark	Rest of Western Europe
DJ	Djibouti	Other
DM	Dominica	Other
DO	Dominican Republic	Rest of Latin America
EC	Ecuador	Rest of Latin America
EG	Egypt	Egypt
SV	El Salvador	Rest of Latin America
GQ	Equatorial Guinea	Other
ER	Eritrea	Rest of Africa
EE	Estonia	Other
ET	Ethiopia	Rest of Africa
SZ	Eswatini	Rest of Africa

Code de pays ISO à deux chiffres	Nom du pays	WhatsApp région de facturation des conversations
FK	Falkland Islands	Other
FO	Faroe Islands	Other
FJ	Fiji	Other
FI	Finland	Rest of Western Europe
FR	France	France
GF	French Guiana	Other
PF	French Polynesia	Other
TF	French Southern Territories	Other
GA	Gabon	Rest of Africa
GM	Gambia	Rest of Africa
GE	Georgia	Rest of Central & Eastern Europe
DE	Germany	Germany
GH	Ghana	Rest of Africa
GI	Gibraltar	Other
GR	Greece	Rest of Central & Eastern Europe
GL	Greenland	Other
GD	Grenada	Other
GP	Guadeloupe	Other
GU	Guam	Other

Code de pays ISO à deux chiffres	Nom du pays	WhatsApp région de facturation des conversations
GT	Guatemala	Rest of Latin America
GG	Guernsey	Other
GN	Guinea	Other
GW	Guinea-Bissau	Rest of Africa
GY	Guyana	Other
HT	Haiti	Rest of Latin America
HM	Heard and McDonald Islands	Other
HN	Honduras	Rest of Latin America
HK	Hong Kong	Rest of Asia Pacific
HU	Hungary	Rest of Central & Eastern Europe
IS	Iceland	Other
IN	India	India
ID	Indonesia	Indonesia
IQ	Iraq	Rest of Middle East
IE	Ireland	Rest of Western Europe
IM	Isle of Man	Other
IL	Israel	Israel
IT	Italy	Italy
JM	Jamaica	Rest of Latin America

Code de pays ISO à deux chiffres	Nom du pays	WhatsApp région de facturation des conversations
JP	Japan	Rest of Asia Pacific
JE	Jersey	Other
JO	Jordan	Rest of Middle East
KZ	Kazakhstan	Other
KE	Kenya	Rest of Africa
KI	Kiribati	Other
XK	Kosovo	Other
KW	Kuwait	Rest of Middle East
KG	Kyrgyzstan	Other
LA	Lao PDR	Rest of Asia Pacific
LV	Latvia	Rest of Central & Eastern Europe
LB	Lebanon	Rest of Middle East
LS	Lesotho	Rest of Africa
LR	Liberia	Rest of Africa
LY	Libya	Rest of Africa
LI	Liechtenstein	Other
LT	Lithuania	Rest of Central & Eastern Europe
LU	Luxembourg	Other
MO	Macao	Other

Code de pays ISO à deux chiffres	Nom du pays	WhatsApp région de facturation des conversations
MK	Macedonia	Rest of Central & Eastern Europe
MG	Madagascar	Rest of Africa
MW	Malawi	Rest of Africa
MY	Malaysia	Malaysia
MV	Maldives	Other
ML	Mali	Rest of Africa
MT	Malta	Other
MH	Marshall Islands	Other
MQ	Martinique	Other
MR	Mauritania	Rest of Africa
MU	Mauritius	Other
YT	Mayotte	Other
MX	Mexico	Mexico
FM	Micronesia	Other
MD	Moldova	Rest of Central & Eastern Europe
MC	Monaco	Other
MN	Mongolia	Rest of Asia Pacific
ME	Montenegro	Other
MS	Montserrat	Other

Code de pays ISO à deux chiffres	Nom du pays	WhatsApp région de facturation des conversations
MA	Morocco	Rest of Africa
MZ	Mozambique	Rest of Africa
MM	Myanmar	Other
NA	Namibia	Rest of Africa
NR	Nauru	Other
NP	Nepal	Rest of Asia Pacific
NL	Netherlands	Netherlands
NC	New Caledonia	Other
NZ	New Zealand	Rest of Asia Pacific
NI	Nicaragua	Rest of Latin America
NE	Niger	Rest of Africa
NG	Nigeria	Nigeria
NU	Niue	Other
NF	Norfolk Island	Other
MP	Northern Mariana Islands	Other
NO	Norway	Rest of Western Europe
OM	Oman	Rest of Middle East
PK	Pakistan	Pakistan
PW	Palau	Other
PS	Palestinian Territory	Other

Code de pays ISO à deux chiffres	Nom du pays	WhatsApp région de facturation des conversations
PA	Panama	Rest of Latin America
PG	Papua New Guinea	Rest of Asia Pacific
PY	Paraguay	Rest of Latin America
PE	Peru	Peru
PH	Philippines	Rest of Asia Pacific
PN	Pitcairn	Other
PL	Poland	Rest of Central & Eastern Europe
PT	Portugal	Rest of Western Europe
PR	Puerto Rico	Rest of Latin America
QA	Qatar	Rest of Middle East
CG	Republic of Congo	Other
RE	Reunion	Other
RO	Romania	Rest of Central & Eastern Europe
RU	Russian Federation	Russia
RW	Rwanda	Rest of Africa
SH	Saint Helena	Other
KN	Saint Kitts and Nevis	Other
LC	Saint Lucia	Other
PM	Saint Pierre and Miquelon	Other

Code de pays ISO à deux chiffres	Nom du pays	WhatsApp région de facturation des conversations
VC	Saint Vincent and Grenadines	Other
BL	Saint-Barthelemy	Other
MF	Saint-Martin	Other
WS	Samoa	Other
SM	San Marino	Other
ST	Sao Tome and Principe	Other
SA	Saudi Arabia	Saudi Arabia
SN	Senegal	Rest of Africa
RS	Serbia	Rest of Central & Eastern Europe
SC	Seychelles	Other
SL	Sierra Leone	Rest of Africa
SG	Singapore	Rest of Asia Pacific
SX	Sint Maarten	Other
SK	Slovakia	Rest of Central & Eastern Europe
SI	Slovenia	Rest of Central & Eastern Europe
SB	Solomon Islands	Other
SO	Somalia	Rest of Africa
ZA	South Africa	South Africa

Code de pays ISO à deux chiffres	Nom du pays	WhatsApp région de facturation des conversations
GS	South Georgia and the South Sandwich Islands	Other
KR	South Korea	Other
SS	South Sudan	Rest of Africa
ES	Spain	Spain
LK	Sri Lanka	Rest of Asia Pacific
SR	Suriname	Other
SJ	Svalbard and Jan Mayen Islands	Other
SE	Sweden	Rest of Western Europe
CH	Switzerland	Rest of Western Europe
TW	Taiwan	Rest of Asia Pacific
TJ	Tajikistan	Rest of Asia Pacific
TZ	Tanzania	Rest of Africa
TH	Thailand	Rest of Asia Pacific
TL	Timor-Leste	Other
TG	Togo	Rest of Africa
TK	Tokelau	Other
TO	Tonga	Other
TT	Trinidad and Tobago	Other
TA	Tristan da Cunha	Other

Code de pays ISO à deux chiffres	Nom du pays	WhatsApp région de facturation des conversations
TN	Tunisia	Rest of Africa
TR	Turkey	Turkey
TM	Turkmenistan	Rest of Asia Pacific
TC	Turks and Caicos Islands	Other
TV	Tuvalu	Other
UG	Uganda	Rest of Africa
UA	Ukraine	Rest of Central & Eastern Europe
AE	United Arab Emirates	United Arab Emirates
GB	United Kingdom	United Kingdom
US	United States	North America
UY	Uruguay	Rest of Latin America
UM	US Minor Outlying Islands	Other
UZ	Uzbekistan	Rest of Asia Pacific
VU	Vanuatu	Other
VA	Vatican City State	Other
VE	Venezuela	Rest of Latin America
VN	Vietnam	Rest of Asia Pacific
VI	Virgin Islands	Other
WF	Wallis and Futuna Islands	Other

Code de pays ISO à deux chiffres	Nom du pays	WhatsApp région de facturation des conversations
EH	Western Sahara	Other
YE	Yemen	Rest of Middle East
ZM	Zambia	Rest of Africa
ZW	Zimbabwe	Other

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

La surveillance joue un rôle important dans le maintien de la fiabilité, de la disponibilité et des performances de AWS End User Messaging Social et de vos autres solutions AWS. AWS fournit les outils de surveillance suivants pour surveiller les messages sociaux des utilisateurs AWS finaux, signaler les problèmes et prendre des mesures automatiques le cas échéant :

- Amazon CloudWatch surveille vos AWS ressources et les applications que vous utilisez 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 CloudWatch suivre l'utilisation du processeur ou d'autres indicateurs de vos EC2 instances Amazon et lancer automatiquement de nouvelles instances en cas de besoin. Pour plus d'informations, consultez le guide de CloudWatch l'utilisateur Amazon.
- Amazon CloudWatch Logs vous permet de surveiller, de stocker et d'accéder à vos fichiers journaux à partir d' EC2 instances Amazon et d'autres sources. CloudTrail 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 plus d'informations, consultez le guide de l'utilisateur d'Amazon CloudWatch Logs.
- AWS CloudTrailcapture les appels d'API et les événements associés effectués par ou pour le compte de votre AWS compte et envoie les fichiers journaux dans un compartiment Amazon S3 que vous spécifiez. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. Pour plus d'informations, consultez le Guide de l'utilisateur AWS CloudTrail.

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

Vous pouvez surveiller l'utilisation des réseaux sociaux par les utilisateurs AWS finaux CloudWatch, qui collectent des données brutes et les traitent en indicateurs lisibles 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 plus d'informations, consultez 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.

> **Note**
>
> Avant de pouvoir utiliser les CloudWatch métriques, vous devez créer un rôle de lien de service.

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

Mesure	Unit	Description
WhatsAppConversationFeeCount	Nombre	Le montant des frais de WhatsApp conversation
WhatsAppMessageFeeCount	Nombre	Le montant des frais de WhatsApp message
MetaTemplateMessageFeeCount	Nombre	Le nombre de frais liés aux méta-modèles de messages

> **Note**
>
> La WhatsAppConversationFeeCount métrique n'est plus disponible à compter du 1er juillet 2025.

Dimension	Description
MessageFeeType	Les types de frais valides sont les suivants : Standard
DestinationCountryCode	Le code ISO à deux lettres du pays
WhatsAppPhoneNumberArn	L'ARN du numéro de téléphone
MetaTemplateMessageFeeType	Les types de frais valides sont les suivants : regular, free_customer_service, free_entry_point
MetaTemplateMessageFeeCategory	Les catégories de frais valides sont les suivantes : service, marketing, utilité, authentification, authentication_international
ConversationFeeType	Les catégories de frais valides sont les suivantes : service, marketing, utilité, authentification, authentication_international

> **Note**
>
> La ConversationFeeType dimension n'est plus disponible à compter du 1er juillet 2025.

Enregistrement des appels de l'API sociale de messagerie de l'utilisateur AWS final à l'aide de AWS CloudTrail

AWS End User Messaging Social est intégré à AWS CloudTrailun service qui fournit un enregistrement des actions entreprises par un utilisateur, un rôle ou un Service AWS. CloudTrail capture tous les appels d'API pour AWS End User Messaging Social sous forme d'événements. Les appels capturés incluent des appels provenant de la console sociale de messagerie de l'utilisateur AWS final et des appels de code vers les opérations de l'API sociale de messagerie de l'utilisateur AWS final. À l'aide des informations collectées par CloudTrail, vous pouvez déterminer la demande qui a été faite à AWS End User Messaging Social, l'adresse IP à partir de laquelle la demande a été faite, la date à laquelle elle a été faite et des informations supplémentaires.

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.
- Si la demande a été faite au nom d'un utilisateur du centre d'identité IAM.
- 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, consultable, téléchargeable et immuable des 90 derniers jours des événements de gestion enregistrés dans un. 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 CloudTrail l'historique des événements est gratuite.

Pour un enregistrement continu des événements de vos 90 Compte AWS derniers jours, créez un magasin de données sur les événements de Trail ou CloudTrailLake.

CloudTrail sentiers

Un suivi permet CloudTrail de fournir des fichiers journaux à un compartiment Amazon S3. Tous les sentiers créés à l'aide du AWS Management Console sont multirégionaux. Vous ne pouvez créer un journal de suivi en une ou plusieurs régions à l'aide de l' AWS CLI. Il est recommandé de créer un parcours multirégional, car vous capturez l'activité dans l'ensemble Régions AWS de votre compte. Si vous créez un journal de suivi pour une seule région, il convient de n'afficher que les événements enregistrés dans le journal de suivi pour une seule région Région AWS. Pour plus d'informations sur les journaux de suivi, consultez Créez un journal de suivi dans vos Compte AWS et Création d'un journal de suivi pour une organisation dans le AWS CloudTrail Guide de l'utilisateur.

Vous pouvez envoyer une copie de vos événements de gestion en cours dans votre compartiment Amazon S3 gratuitement CloudTrail en créant un journal. Toutefois, des frais de stockage Amazon S3 sont facturés. 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 Stockages de données sur les événements du lac

CloudTrail Lake vous permet d'exécuter des requêtes SQL sur vos événements. CloudTrail Lake convertit les événements existants au format JSON basé sur les lignes au format Apache ORC. ORC 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 stockages et requêtes de données sur les événements de Lake entraînent des coûts. 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, CloudTrail n'enregistre pas les événements liés aux données. 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 AWS CLI des opérations de CloudTrail l'API. Pour plus d'informations sur la façon de journaliser les événements de données, consultez Journalisation des événements de données avec la AWS Management Console et Journalisation des événements de données avec l' AWS Command Line Interface dans le Guide de l'utilisateur AWS CloudTrail .

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 appels d'API 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 champs `eventName`, `readOnly` et `resources.ARN` afin de ne journaliser que les événements importants pour vous. Pour plus d'informations sur ces champs, voir AdvancedFieldSelector dans la Référence d'API AWS CloudTrail

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

Les événements de gestion fournissent des informations sur les opérations de gestion effectuées sur les ressources de votre Compte AWS. Ils sont également connus sous le nom opérations de plan de contrôle. Par défaut, CloudTrail enregistre 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 AWS liste des opérations du plan de contrôle social de la messagerie des utilisateurs AWS finaux auxquelles End User Messaging Social se connecte CloudTrail, consultez la référence de l'API sociale de messagerie des utilisateurs AWS finaux.

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

Un événement représente une demande unique provenant de n'importe quelle source et inclut des informations sur l'opération d'API demandée, la date et l'heure de l'opération, les paramètres de la demande, etc. CloudTrail les fichiers journaux ne constituent pas une trace ordonnée des appels d'API publics. Les événements n'apparaissent donc pas dans un ordre spécifique.

L'exemple suivant montre un CloudTrail événement illustrant 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 susceptibles de vous aider à améliorer l'engagement de vos clients et à 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
- Obtenir une autorisation
- Contenu de message interdit
- Effectuer un audit de vos listes de clients
- Ajuster votre envoi en fonction de l'implication
- Envoyer à des heures appropriées

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. Conservez les informations d'inscription 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 à l'aide d'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 envoyez un message avec WhatsApp, suivez 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 stratagèmes	• Work-from-home programmes • Opportunités d'investissement à faible risque • Schémas de marketing pyramidaux ou multi-niveaux

Catégorie	Exemples
Substances illégales	• Cannabis/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 pendant les heures ouvrables normales de jour. Si vous envoyez des messages à l'heure du dîner ou en pleine nuit, il y a de fortes chances que vos clients se désinscrivent de vos listes pour ne pas être dérangés. Vous voudrez peut-être éviter d'envoyer WhatsApp des messages lorsque vos clients ne peuvent pas y répondre immédiatement.

Sécurité dans AWS la messagerie sociale des utilisateurs finaux

La sécurité du cloud AWS est la priorité absolue. En tant que AWS client, vous bénéficiez de centres de données et d'architectures réseau conçus pour répondre aux exigences des entreprises les plus sensibles en matière de sécurité.

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

- Sécurité du cloud : AWS est chargée de protéger l'infrastructure qui exécute les AWS services dans le AWS Cloud. 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 cadre des programmes de AWS conformité Programmes de de conformité. Pour en savoir plus sur les programmes de conformité qui s'appliquent à AWS la messagerie sociale destinée aux utilisateurs finaux, voir AWS Services concernés par 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 AWS End User Messaging Social. Les rubriques suivantes expliquent comment configurer AWS End User Messaging Social pour répondre à vos objectifs de sécurité et de conformité. Vous apprendrez également à utiliser d'autres AWS services qui vous aident à surveiller et à sécuriser les ressources sociales de messagerie de vos utilisateurs AWS finaux.

Rubriques

- Protection des données dans les réseaux sociaux destinés aux utilisateurs AWS finaux
- Gestion des identités et des accès pour AWS la messagerie sociale des utilisateurs finaux
- Validation de conformité pour les utilisateurs AWS finaux Messaging Social
- Résilience dans AWS la messagerie sociale destinée aux utilisateurs finaux
- Sécurité de l'infrastructure dans les réseaux sociaux destinés aux utilisateurs AWS finaux
- Prévention du cas de figure de l'adjoint désorienté entre services
- Bonnes pratiques de sécurité

- Utilisation de rôles liés à un service pour la messagerie sociale de l'utilisateur AWS final

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 chargé de protéger l'infrastructure mondiale qui gère tous les 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, consultez Questions fréquentes (FAQ) sur la confidentialité des données. Pour en savoir plus sur la protection des données en Europe, consultez le billet de blog Modèle de responsabilité partagée AWS et RGPD (Règlement général sur la protection des données) sur le Blog de sécuritéAWS .

À des fins de protection des données, nous vous recommandons de protéger les Compte AWS informations d'identification et de configurer les utilisateurs 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 (MFA) avec chaque compte.
- SSL/TLS À utiliser pour communiquer avec AWS les ressources. Nous exigeons TLS 1.2 et recommandons TLS 1.3.
- Configurez l'API et la journalisation de l'activité des utilisateurs 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 qu'ils contiennent 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 modules cryptographiques validés par la norme FIPS 140-3 pour accéder AWS via une interface de ligne de commande ou une API, utilisez un point de terminaison FIPS. Pour plus d'informations sur les points de terminaison FIPS disponibles, consultez Norme FIPS (Federal Information Processing Standard) 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 console, de l'API ou AWS SDKs. AWS CLI 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 une adresse URL à un serveur externe, nous vous recommandons fortement de ne pas inclure d'informations d'identification dans l'adresse URL permettant de valider votre demande adressée à ce 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 cryptées en transit et au repos à l'intérieur des AWS limites. Lorsque vous soumettez des données à AWS End User Messaging Social, celui-ci crypte les données au fur et à mesure de leur réception et les stocke. Lorsque vous récupérez des données auprès de AWS End User Messaging Social, celui-ci vous les transmet en utilisant les protocoles de sécurité actuels.

Chiffrement au repos

AWS End User Messaging Social chiffre toutes les données qu'il stocke pour vous à l'intérieur des 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 internes AWS Key Management Service (AWS KMS) 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 End User Messaging Social utilise le protocole HTTPS et le protocole TLS (Transport Layer Security) 1.2 pour communiquer avec vos clients, vos applications et Meta. Pour communiquer avec

d'autres AWS services, AWS End User Messaging Social utilise le protocole HTTPS et le protocole TLS 1.2. En outre, lorsque vous créez et gérez des ressources sociales de messagerie pour les utilisateurs AWS finaux à l'aide de la console, d'un AWS SDK ou du AWS Command Line Interface, toutes les communications sont sécurisées à l'aide du protocole HTTPS et du protocole 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 fournir et utiliser vos propres clés AWS KMS ou d'autres clés pour chiffrer les données que vous stockez dans AWS End User Messaging Social.

Confidentialité du trafic inter-réseaux

La confidentialité du trafic interréseau fait référence à la sécurisation des connexions et du trafic entre AWS End User Messaging Social et vos clients et applications locaux, ainsi qu'entre AWS End User Messaging Social et les autres AWS ressources du même réseau. Région AWS Les fonctionnalités et pratiques suivantes peuvent vous aider à garantir la confidentialité du trafic interréseau pour les utilisateurs AWS finaux de Messaging Social.

Trafic entre l'utilisateur AWS final Messaging Social et les clients et applications locaux

Pour établir une connexion privée entre AWS End User Messaging Social et les clients et applications de votre réseau local, 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 End User Messaging Social par le biais de la publication APIs, nous vous recommandons de respecter les exigences relatives à la messagerie sociale des utilisateurs AWS finaux pour les appels d'API. AWS End User Messaging Social exige que les clients utilisent le protocole TLS (Transport Layer Security) 1.2 ou version ultérieure. Les clients doivent également prendre en charge les suites de chiffrement PFS (Perfect Forward Secrecy) comme Ephemeral Diffie-Hellman (DHE) ou Elliptic Curve Ephemeral 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 identifiant de clé d'accès et d'une clé d'accès secrète associés à un principal AWS Identity and Access Management (IAM) de 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 la messagerie sociale des utilisateurs finaux

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. Les administrateurs IAM contrôlent qui peut être authentifié (connecté) et autorisé (autorisé) à utiliser les ressources sociales de messagerie des utilisateurs AWS finaux. IAM est un Service AWS outil que vous pouvez utiliser sans frais supplémentaires.

Rubriques

- Public ciblé
- Authentification par des identités
- Gestion des accès à l'aide de politiques
- Comment fonctionne AWS Final User Messaging Social avec IAM
- Exemples de politiques basées sur l'identité pour les utilisateurs AWS finaux Messaging Social
- AWS politiques gérées pour la messagerie sociale des utilisateurs AWS finaux
- Résolution des problèmes liés AWS à l'identité et à l'accès aux réseaux sociaux des utilisateurs finaux

Public ciblé

La façon dont vous utilisez AWS Identity and Access Management (IAM) varie en fonction du travail que vous effectuez dans AWS End User Messaging Social.

Utilisateur du service : si vous utilisez le service social de messagerie utilisateur AWS final pour effectuer votre travail, votre administrateur vous fournit les informations d'identification et les autorisations dont vous avez besoin. Au fur et à mesure que vous utilisez de plus en plus de fonctionnalités sociales de messagerie pour les utilisateurs AWS finaux dans le cadre de votre travail, vous aurez peut-être 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, consultezRésolution des problèmes liés AWS à l'identité et à l'accès aux réseaux sociaux des utilisateurs finaux.

Administrateur du service — Si vous êtes responsable des ressources sociales de messagerie pour les utilisateurs AWS finaux au sein de votre entreprise, vous avez probablement un accès complet à AWS End User Messaging Social. C'est à vous de déterminer les fonctionnalités et ressources sociales de messagerie destinées aux utilisateurs AWS finaux auxquelles les utilisateurs de vos services doivent accéder. Vous devez ensuite soumettre les demandes à votre administrateur IAM 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 manière dont votre entreprise peut utiliser IAM avec AWS End User Messaging Social, consultezComment fonctionne AWS Final User Messaging Social avec IAM.

Administrateur IAM : si vous êtes administrateur IAM, vous souhaiterez peut-être en savoir plus sur la manière dont vous pouvez rédiger des politiques pour gérer l'accès à AWS End User Messaging Social. Pour consulter des exemples de politiques basées sur l'identité sociale de messagerie à l'utilisateur AWS final que vous pouvez utiliser dans IAM, consultez. Exemples de politiques basées sur l'identité pour les utilisateurs AWS finaux Messaging Social

Authentification par des identités

L'authentification est la façon dont vous vous connectez à AWS l'aide de vos informations d'identification. Vous devez être authentifié (connecté à AWS) en tant qu'utilisateur IAM ou en assumant un rôle IAM. Utilisateur racine d'un compte AWS

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

Selon le type d'utilisateur que vous êtes, vous pouvez vous connecter au portail 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 y accédez AWS par programmation, AWS fournit un kit de développement logiciel (SDK) et une interface de ligne de commande (CLI) pour signer cryptographiquement vos demandes à l'aide de vos informations d'identification. Si vous n'utilisez pas d' AWS outils, vous devez signer vous-même les demandes. Pour plus d'informations sur l'utilisation de la méthode recommandée pour

signer des demandes vous-même, consultez AWS Signature Version 4 pour les demandes d'API dans le Guide de l'utilisateur IAM.

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

Compte AWS utilisateur root

Lorsque vous créez un Compte AWS, vous commencez par une identité de connexion unique qui donne un accès complet à toutes Services AWS les ressources du compte. Cette identité est appelée utilisateur Compte AWS root et est accessible en vous connectant avec l'adresse e-mail et le 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 racine, consultez Tâches nécessitant des informations d'identification d'utilisateur racine dans le Guide de l'utilisateur IAM.

Identité fédérée

La meilleure pratique consiste à obliger les utilisateurs humains, y compris ceux qui ont besoin d'un accès administrateur, à utiliser la fédération avec un fournisseur d'identité pour accéder à l'aide Services AWS d'informations d'identification temporaires.

Une identité fédérée est un utilisateur de l'annuaire des utilisateurs de votre entreprise, d'un fournisseur d'identité Web AWS Directory Service, du répertoire Identity Center ou de tout utilisateur qui y accède à l'aide des informations d'identification fournies Services AWS par le biais d'une source d'identité. Lorsque des identités fédérées y accèdent Comptes AWS, elles assument des rôles, qui fournissent 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 pouvez vous connecter et synchroniser avec un ensemble d'utilisateurs et de groupes dans votre propre source d'identité afin de les utiliser dans toutes vos applications Comptes AWS et applications. Pour obtenir des informations sur IAM Identity Center, consultez Qu'est-ce que IAM Identity Center ? dans le Guide de l'utilisateur AWS IAM Identity Center .

Utilisateurs et groupes IAM

Un utilisateur IAM est une identité au sein de vous Compte AWS qui possède des autorisations spécifiques pour une seule personne ou une seule application. Dans la mesure du possible, nous vous recommandons de vous appuyer sur des informations d'identification temporaires plutôt que de créer des utilisateurs IAM ayant des informations d'identification à long terme telles que des mots de passe et des clés d'accès. Toutefois, si certains cas d'utilisation spécifiques nécessitent des informations d'identification à long terme avec les utilisateurs IAM, nous vous recommandons d'effectuer une rotation des clés d'accès. Pour plus d'informations, consultez Rotation régulière des clés d'accès pour les cas d'utilisation nécessitant des informations d'identification dans le Guide de l'utilisateur IAM.

Un groupe IAM est une identité qui concerne un ensemble d'utilisateurs IAM. 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 nommer un groupe IAMAdminset lui donner les autorisations nécessaires pour administrer les ressources IAM.

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 plus d'informations, consultez Cas d'utilisation pour les utilisateurs IAM dans le Guide de l'utilisateur IAM.

Rôles IAM

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

Les rôles IAM 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

obtenir des informations sur les rôles pour la fédération, consultez Création d'un rôle pour un fournisseur d'identité tiers (fédération) dans le Guide de l'utilisateur IAM. Si vous utilisez IAM Identity Center, vous configurez un jeu d'autorisations. IAM Identity Center met en corrélation le jeu d'autorisations avec un rôle dans IAM afin de contrôler à quoi vos identités peuvent accéder après leur authentification. Pour plus d'informations sur les jeux d'autorisations, consultez Jeux d'autorisations dans le Guide de l'utilisateur AWS IAM Identity Center .

- Autorisations d'utilisateur IAM temporaires : un rôle ou un utilisateur IAM peut endosser un rôle IAM pour profiter temporairement d'autorisations différentes pour une tâche spécifique.
- Accès intercompte : vous pouvez utiliser un rôle IAM pour permettre à un utilisateur (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, dans certains Services AWS cas, vous pouvez associer une politique directement à une ressource (au lieu d'utiliser un rôle comme 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 dans IAM dans le Guide de l'utilisateur IAM.
- Accès multiservices — 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.
  - Sessions d'accès direct (FAS) : lorsque vous utilisez un utilisateur ou un rôle IAM pour effectuer des actions AWS, vous êtes considéré comme un mandant. Lorsque vous utilisez certains services, vous pouvez effectuer une action qui initie une autre action dans un autre service. FAS utilise les autorisations du principal appelant et Service AWS, associées Service AWS à la demande, pour adresser des demandes aux services en aval. Les demandes FAS ne sont effectuées que lorsqu'un service reçoit une demande qui nécessite des interactions avec d'autres personnes Services AWS ou des ressources pour être traitée. Dans ce cas, vous devez disposer d'autorisations nécessaires pour effectuer les deux actions. Pour plus de détails sur une politique lors de la formulation de demandes FAS, consultez Transmission des sessions d'accès.
  - Rôle de service : il s'agit d'un rôle IAM attribué à un service afin de réaliser des actions en votre nom. Un administrateur IAM peut créer, modifier et supprimer un rôle de service à partir d'IAM. Pour plus d'informations, consultez Création d'un rôle pour la délégation d'autorisations à un Service AWS dans le Guide de l'utilisateur IAM.
  - Rôle lié à un service — Un rôle lié à un 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 apparaissent dans votre Compte AWS répertoire et appartiennent au service. Un administrateur IAM 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 rôle IAM pour gérer les informations d'identification temporaires pour les applications qui s'exécutent sur une EC2 instance et qui envoient des demandes AWS CLI d' AWS API. Cela est préférable au stockage des clés d'accès dans l' EC2 instance. Pour attribuer un AWS rôle à une EC2 instance et le rendre disponible pour toutes ses applications, vous devez créer un profil d'instance attaché à l'instance. Un profil d'instance contient le rôle et permet aux programmes exécutés sur l' EC2 instance d'obtenir des informations d'identification temporaires. Pour plus d'informations, consultez Utiliser un rôle IAM pour accorder des autorisations aux applications exécutées sur des EC2 instances Amazon dans le guide de l'utilisateur IAM.

Gestion des accès à l'aide de politiques

Vous contrôlez l'accès en AWS créant des politiques et en les associant à AWS des identités ou à des ressources. Une politique est un objet AWS qui, lorsqu'il est associé à une identité ou à une ressource, définit leurs autorisations. AWS évalue ces politiques lorsqu'un principal (utilisateur, utilisateur root ou session de rôle) fait une demande. Les autorisations dans les politiques déterminent si la demande est autorisée ou refusée. La plupart des politiques sont stockées AWS sous forme de documents JSON. Pour plus d'informations sur la structure et le contenu des documents de politique JSON, consultez Vue d'ensemble des politiques JSON dans le Guide de l'utilisateur IAM.

Les administrateurs peuvent utiliser les politiques AWS JSON 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 administrateur IAM peut créer des politiques IAM. L'administrateur peut ensuite ajouter les politiques IAM aux rôles et les utilisateurs peuvent assumer les rôles.

Les politiques IAM 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 appliquant cette politique peut obtenir des informations sur le rôle à partir de AWS Management Console AWS CLI, de ou de l' AWS API.

Politiques basées sur l'identité

Les politiques basées sur l'identité sont des documents de politique d'autorisations JSON que vous pouvez attacher à une identité telle qu'un utilisateur, un groupe d'utilisateurs ou un rôle IAM. 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 politique basée sur l'identité, consultez Définition d'autorisations IAM personnalisées avec des politiques gérées par le client dans le Guide de l'utilisateur IAM.

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 associer à plusieurs utilisateurs, groupes et rôles au sein de votre Compte AWS. Les politiques gérées incluent les politiques AWS gérées et les politiques gérées par le client. Pour découvrir comment choisir entre une politique gérée et une politique en ligne, consultez Choix entre les politiques gérées et les politiques en ligne dans le Guide de l'utilisateur IAM.

Politiques basées sur les ressources

Les politiques basées sur les ressources sont des documents de politique JSON que vous attachez à une ressource. Par exemple, les politiques de confiance de rôle IAM et les politiques de compartiment Amazon S3 sont des politiques basées sur les ressources. 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 principaux peuvent inclure des comptes, des utilisateurs, des rôles, des utilisateurs fédérés ou. Services AWS

Les politiques basées sur les ressources sont des politiques en ligne situées dans ce service. Vous ne pouvez pas utiliser les politiques AWS gérées par IAM dans une stratégie basée sur les ressources.

Listes de contrôle d'accès (ACLs)

Les listes de contrôle d'accès (ACLs) contrôlent les principaux (membres du compte, utilisateurs ou rôles) autorisés à accéder à une ressource. ACLs sont similaires aux politiques basées sur les ressources, bien qu'elles n'utilisent pas le format de document de politique JSON.

Amazon S3 et AWS WAF Amazon VPC sont des exemples de services compatibles. ACLs Pour en savoir plus ACLs, consultez la 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 politiques moins courants. 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 entité IAM (utilisateur ou rôle IAM). 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 plus d'informations sur les limites d'autorisations, consultez Limites d'autorisations pour des entités IAM dans le Guide de l'utilisateur IAM.
- Politiques de contrôle des services (SCPs) : SCPs politiques JSON qui spécifient les autorisations maximales pour une organisation ou une unité organisationnelle (UO) dans AWS Organizations. AWS Organizations est un service permettant de regrouper et de gérer de manière centralisée Comptes AWS les multiples propriétés de votre entreprise. Si vous activez toutes les fonctionnalités d'une organisation, vous pouvez appliquer des politiques de contrôle des services (SCPs) à l'un ou à l'ensemble de vos comptes. Le SCP limite les autorisations pour les entités figurant dans les comptes des membres, y compris chacune Utilisateur racine d'un compte AWS d'entre elles. 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 contrôle des ressources (RCPs) : RCPs politiques JSON que vous pouvez utiliser pour définir le maximum d'autorisations disponibles pour les ressources de vos comptes sans mettre à jour les politiques IAM associées à chaque ressource que vous possédez. Le RCP limite les autorisations pour les ressources des comptes membres et peut avoir un impact sur les autorisations effectives pour les identités, y compris Utilisateur racine d'un compte AWS, qu'elles appartiennent ou non à votre organisation. Pour plus d'informations sur les Organizations RCPs, y compris une liste de ces Services AWS supports RCPs, consultez la section Resource control policies (RCPs) 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 Politiques de session dans le Guide de l'utilisateur IAM.

Plusieurs types de politique

Lorsque plusieurs types de politiques s'appliquent à la requête, les autorisations en résultant sont plus compliquées à comprendre. Pour savoir comment AWS déterminer s'il faut autoriser une demande lorsque plusieurs types de politiques sont impliqués, consultez la section Logique d'évaluation des politiques dans le guide de l'utilisateur IAM.

Comment fonctionne AWS Final User Messaging Social avec IAM

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

Fonctionnalités IAM que vous pouvez utiliser avec AWS End User Messaging Social

Fonctionnalité IAM	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 (identifications dans les politiques)	Partielle

Fonctionnalité IAM	AWS Messagerie à l'utilisateur final Assistance sociale
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 dont les services de messagerie sociale destinés aux utilisateurs AWS finaux et les autres AWS services fonctionnent avec la plupart des fonctionnalités IAM, consultez la section AWS Services compatibles avec IAM dans le guide de l'utilisateur IAM.

Politiques basées sur l'identité pour les utilisateurs AWS finaux Messaging Social

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

Les politiques basées sur l'identité sont des documents de politique d'autorisations JSON que vous pouvez attacher à une identité telle qu'un utilisateur, un groupe d'utilisateurs ou un rôle IAM. 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 politique basée sur l'identité, consultez Définition d'autorisations IAM personnalisées avec des politiques gérées par le client dans le Guide de l'utilisateur IAM.

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 découvrir tous les éléments que vous utilisez dans une politique JSON, consultez Références des éléments de politique JSON IAM dans le Guide de l'utilisateur IAM.

Exemples de politiques basées sur l'identité pour les utilisateurs AWS finaux Messaging Social

Pour consulter des exemples de politiques basées sur l'identité sociale relatives à la messagerie à l'utilisateur AWS final, consultez. Exemples de politiques basées sur l'identité pour les utilisateurs AWS finaux Messaging Social

Politiques basées sur les ressources au sein de AWS End User Messaging Social

Prend en charge les politiques basées sur les ressources : non

Les politiques basées sur les ressources sont des documents de politique JSON que vous attachez à une ressource. Par exemple, les politiques de confiance de rôle IAM et les politiques de compartiment Amazon S3 sont des politiques basées sur les ressources. 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 principaux peuvent inclure des comptes, des utilisateurs, des rôles, des utilisateurs fédérés ou. Services AWS

Pour permettre un accès intercompte, vous pouvez spécifier un compte entier ou des entités IAM dans un autre compte en tant que principal dans une politique basée sur les ressources. L'ajout d'un principal intercompte à une politique basée sur les ressources ne représente qu'une partie de l'instauration de la relation d'approbation. Lorsque le principal et la ressource sont différents Comptes AWS, un administrateur IAM du compte sécurisé doit également accorder à l'entité principale (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 Accès intercompte aux ressources dans IAM dans le Guide de l'utilisateur IAM.

Actions stratégiques pour la messagerie sociale destinée aux utilisateurs AWS finaux

Prend en charge les actions de politique : oui

Les administrateurs peuvent utiliser les politiques AWS JSON 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 `Action` d'une politique JSON décrit les actions que vous pouvez utiliser pour autoriser ou refuser l'accès à une politique. Les actions de stratégie portent généralement le même nom que l'opération AWS d'API associée. Il existe quelques exceptions, telles que les actions avec autorisations uniquement qui n'ont pas d'opération API correspondante. 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 politique 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 consulter des exemples de politiques basées sur l'identité sociale relatives à la messagerie à l'utilisateur AWS final, consultez. Exemples de politiques basées sur l'identité pour les utilisateurs AWS finaux Messaging Social

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 les politiques AWS JSON 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 de politique JSON `Resource` indique 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 caractéristiques ARNs, consultez la section Ressources définies par AWS End User Messaging Social dans la référence d'autorisation de service. Pour savoir avec quelles actions vous pouvez spécifier l'ARN de chaque ressource, voir Actions définies par l'utilisateur AWS final Messaging Social.

Pour consulter des exemples de politiques basées sur l'identité sociale relatives à la messagerie à l'utilisateur AWS final, consultez. Exemples de politiques basées sur l'identité pour les utilisateurs AWS finaux Messaging Social

Clés de conditions de politique pour les messages sociaux destinés aux utilisateurs AWS finaux

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

Les administrateurs peuvent utiliser les politiques AWS JSON 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 utilisateur IAM l'autorisation d'accéder à une ressource

uniquement si elle est balisée avec son nom d'utilisateur IAM. Pour plus d'informations, consultez Éléments d'une politique IAM : variables et identifications dans le Guide de l'utilisateur IAM.

AWS prend en charge les clés de condition globales et les clés de condition spécifiques au service. Pour voir toutes les clés de condition AWS globales, voir les clés de contexte de condition AWS globales dans le guide de l'utilisateur IAM.

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, voir Actions définies par l'utilisateur AWS final Messaging Social.

Pour consulter des exemples de politiques basées sur l'identité sociale relatives à la messagerie à l'utilisateur AWS final, consultez. Exemples de politiques basées sur l'identité pour les utilisateurs AWS finaux Messaging Social

ACLs Messagerie sociale pour les utilisateurs AWS finaux

Supports ACLs : Non

Les listes de contrôle d'accès (ACLs) contrôlent les principaux (membres du compte, utilisateurs ou rôles) autorisés à accéder à une ressource. ACLs sont similaires aux politiques basées sur les ressources, bien qu'elles n'utilisent pas le format de document de politique JSON.

ABAC avec messagerie sociale pour les utilisateurs AWS finaux

Prend en charge ABAC (identifications dans les politiques) : partiellement

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

L'ABAC est utile dans les environnements qui connaissent une croissance rapide et pour les cas où la gestion des politiques 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'informations sur ABAC, consultez Définition d'autorisations avec l'autorisation ABAC dans le Guide de l'utilisateur IAM. Pour accéder à un didacticiel décrivant les étapes de configuration de l'ABAC, consultez Utilisation du contrôle d'accès par attributs (ABAC) dans le Guide de l'utilisateur IAM.

Utilisation d'informations d'identification temporaires avec AWS End User Messaging Social

Prend en charge les informations d'identification temporaires : oui

Certains Services AWS ne fonctionnent pas lorsque 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 d'IAM dans le guide de l'utilisateur d'IAM.

Vous utilisez des informations d'identification temporaires si vous vous connectez à l' AWS Management Console aide d'une méthode autre qu'un nom d'utilisateur et un mot de passe. Par exemple, lorsque vous accédez à AWS l'aide du lien d'authentification unique (SSO) de votre entreprise, 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 Passage d'un rôle utilisateur à un rôle IAM (console) dans le Guide de l'utilisateur IAM.

Vous pouvez créer manuellement des informations d'identification temporaires à l'aide de l' AWS API AWS CLI or. Vous pouvez ensuite utiliser ces informations d'identification temporaires pour y accéder AWS. AWS recommande de générer dynamiquement des informations d'identification temporaires 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 principales interservices pour la messagerie sociale des utilisateurs AWS finaux

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

Lorsque vous utilisez un utilisateur ou un rôle IAM pour effectuer des actions AWS, vous êtes considéré comme un mandant. Lorsque vous utilisez certains services, vous pouvez effectuer une action qui initie une autre action dans un autre service. FAS utilise les autorisations du principal appelant et Service AWS, associées Service AWS à la demande, pour adresser des demandes aux services en aval. Les demandes FAS ne sont effectuées que lorsqu'un service reçoit une demande qui nécessite des interactions avec d'autres personnes Services AWS ou des ressources pour être traitée. Dans ce cas, vous devez disposer d'autorisations nécessaires pour effectuer les deux actions. Pour plus de détails sur une politique lors de la formulation de demandes FAS, consultez Transmission des sessions d'accès.

Rôles de service pour l'utilisateur AWS final Messaging Social

Prend en charge les rôles de service : oui

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

> **Warning**
>
> La modification des autorisations associées à un rôle de service peut perturber la fonctionnalité sociale de messagerie de l'utilisateur AWS final. Modifiez les rôles de service uniquement lorsque AWS End User Messaging Social fournit des instructions à cet effet.

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 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 apparaissent dans votre Compte AWS répertoire et appartiennent au service. Un administrateur IAM 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 Services AWS 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 les utilisateurs AWS finaux Messaging Social

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

Pour apprendre à créer une politique basée sur l'identité IAM à l'aide de ces exemples de documents de politique JSON, consultez Création de politiques IAM (console) dans le Guide de l'utilisateur IAM.

Pour plus de détails sur les actions et les types de ressources définis par AWS End User Messaging Social, y compris le ARNs format de chaque type de ressource, voir Actions, ressources et clés de condition pour l'utilisateur AWS final Messaging Social dans la référence d'autorisation du 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 quelqu'un peut créer, accéder ou supprimer des ressources sociales de messagerie utilisateur AWS final 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 du moindre privilège : pour commencer à accorder des autorisations à vos utilisateurs et à vos charges de travail, utilisez les politiques 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 davantage les autorisations en définissant des politiques gérées par les AWS clients spécifiques à vos cas d'utilisation. Pour plus d'informations, consultez politiques gérées par AWS ou politiques gérées par AWS pour les activités professionnelles dans le Guide de l'utilisateur IAM.

- Accordez les autorisations de moindre privilège : lorsque vous définissez des autorisations avec des politiques IAM, 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 d'IAM pour appliquer des autorisations, consultez politiques et autorisations dans IAM dans le Guide de l'utilisateur IAM.
- Utilisez des conditions dans les politiques IAM 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 politique pour spécifier que toutes les demandes doivent être envoyées via SSL. Vous pouvez également utiliser des conditions pour accorder l'accès aux actions de service si elles sont utilisées par le biais d'un service spécifique Service AWS, tel que AWS CloudFormation. Pour plus d'informations, consultez Conditions pour éléments de politique JSON IAM dans le Guide de l'utilisateur IAM.
- Utilisez l'Analyseur d'accès IAM pour valider vos politiques IAM afin de garantir des autorisations sécurisées et fonctionnelles : l'Analyseur d'accès IAM valide les politiques nouvelles et existantes de manière à ce que les politiques IAM respectent le langage de politique IAM (JSON) et les bonnes pratiques IAM. IAM Access 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 Validation de politiques avec IAM Access Analyzer dans le Guide de l'utilisateur IAM.
- Exiger l'authentification multifactorielle (MFA) : si vous avez un scénario qui nécessite des utilisateurs IAM ou un utilisateur root, activez l'authentification MFA pour une sécurité accrue. Compte AWS Pour exiger la MFA lorsque des opérations d'API sont appelées, ajoutez des conditions MFA à vos politiques. Pour plus d'informations, consultez Sécurisation de l'accès aux API avec MFA dans le Guide de l'utilisateur IAM.

Pour plus d'informations sur les bonnes pratiques dans IAM, consultez Bonnes pratiques de sécurité dans IAM dans le Guide de l'utilisateur IAM.

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 d'afficher des informations détaillées sur les ressources sociales de messagerie destinées aux utilisateurs AWS finaux de 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.

Il n'est pas nécessaire d'accorder des autorisations de console minimales aux utilisateurs qui appellent uniquement l'API AWS CLI ou l' AWS API. Autorisez plutôt l'accès à uniquement aux actions qui correspondent à l'opération d'API 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 Ajout d'autorisations à un utilisateur dans le Guide de l'utilisateur IAM.

Autorisation accordée aux utilisateurs pour afficher leurs propres autorisations

Cet exemple montre comment créer une politique qui permet aux utilisateurs IAM d'afficher les politiques en ligne et gérées attachées à leur identité d'utilisateur. Cette politique inclut les autorisations permettant d'effectuer cette action sur la console ou par programmation à l'aide de l'API AWS CLI or AWS .

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
```

```
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS politiques gérées pour la messagerie sociale des utilisateurs AWS finaux

Pour ajouter des autorisations aux utilisateurs, aux groupes et aux rôles, il est plus facile d'utiliser des politiques AWS gérées que de les rédiger vous-même. Il faut du temps et de l'expertise pour créer des politiques gérées par le client IAM qui ne fournissent à votre équipe que les autorisations dont elle a besoin. Pour démarrer rapidement, vous pouvez utiliser nos politiques 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 l'utilisateur IAM.

AWS les services maintiennent et mettent à jour les politiques AWS gérées. Vous ne pouvez pas modifier les autorisations dans les politiques AWS gérées. 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. Les mises à jour des politiques n'endommageront donc pas vos autorisations existantes.

En outre, AWS prend en charge les politiques gérées pour les fonctions professionnelles qui couvrent plusieurs services. Par exemple, la politique ReadOnlyAccess AWS gérée fournit un accès en lecture seule à tous les AWS services et ressources. Lorsqu'un service lance une nouvelle fonctionnalité, il AWS ajoute des autorisations en lecture seule pour les nouvelles opérations et ressources. Pour

obtenir la liste des politiques de fonctions professionnelles et leurs descriptions, consultez la page politiques gérées par AWS pour les fonctions de tâche dans le Guide de l'utilisateur IAM.

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

Consultez les détails des mises à jour apportées aux politiques AWS gérées pour AWS End User Messaging Social depuis que ce service a commencé à suivre ces modifications. Pour recevoir des alertes automatiques concernant les modifications apportées à cette page, abonnez-vous au flux RSS sur la page d'historique des documents sociaux de messagerie destinés aux utilisateurs AWS finaux.

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 apportées AWS à ses politiques gérées.	10 octobre 2024

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

Utilisez les informations suivantes pour vous aider à diagnostiquer et à résoudre les problèmes courants que vous pouvez rencontrer lors de l'utilisation de AWS End User Messaging Social et IAM.

Rubriques

- Je ne suis pas autorisé à effectuer une action dans AWS End User Messaging Social
- Je ne suis pas autorisé à effectuer iam : PassRole
- Je souhaite autoriser des personnes extérieures à moi Compte AWS à accéder à mes ressources sociales de messagerie pour utilisateurs AWS finaux

Je ne suis pas autorisé à effectuer une action dans AWS End User Messaging Social

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 quand l'utilisateur IAM `mateojackson` tente d'utiliser la console pour afficher des informations détaillées sur une ressource *`my-example-widget`* fictive, mais ne dispose pas des autorisations `social-messaging:`*`GetWidget`* fictives.

```
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 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 iam : PassRole

Si vous recevez un message d'erreur indiquant que vous n'êtes pas autorisé à effectuer l'`iam:PassRole`action, vos politiques doivent être mises à jour pour vous permettre de transmettre un rôle à AWS End User 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 un 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 utilisateur IAM nommé `marymajor` essaie d'utiliser la console pour effectuer 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 besoin d'aide, contactez votre AWS administrateur. Votre administrateur vous a fourni vos informations d'identification de connexion.

Je souhaite autoriser des personnes extérieures à moi Compte AWS à accéder à mes ressources sociales de messagerie pour 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 politiques basées sur les ressources ou les listes de contrôle d'accès (ACLs), vous pouvez utiliser ces politiques pour autoriser les utilisateurs à accéder à vos ressources.

Pour plus d'informations, consultez les éléments suivants :

- Pour savoir si AWS End User Messaging Social prend en charge ces fonctionnalités, consultezComment fonctionne AWS Final User Messaging Social avec IAM.
- Pour savoir comment fournir l'accès à vos ressources sur celles Comptes AWS que vous possédez, consultez la section Fournir l'accès à un utilisateur IAM dans un autre utilisateur Compte AWS que vous possédez dans le Guide de l'utilisateur IAM.
- Pour savoir comment fournir l'accès à vos ressources à des tiers Comptes AWS, consultez la section Fournir un accès à des ressources Comptes AWS détenues par des tiers dans le guide de l'utilisateur IAM.
- Pour savoir comment fournir un accès par le biais de la fédération d'identité, consultez Fournir un accès à des utilisateurs authentifiés en externe (fédération d'identité) dans le Guide de l'utilisateur IAM.
- 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 dans IAM dans le Guide de l'utilisateur IAM.

Validation de conformité pour les utilisateurs AWS finaux Messaging Social

Pour savoir si un programme Services AWS de conformité Service AWS s'inscrit dans le champ d'application de programmes de conformité spécifiques, consultez Services AWS la section 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 tiers à l'aide de AWS Artifact. Pour plus d'informations, voir Téléchargement de rapports dans AWS Artifact .

Votre responsabilité en matière de conformité lors de l'utilisation Services AWS est déterminée par la sensibilité de vos données, les objectifs de conformité de votre entreprise et les lois et réglementations applicables. AWS fournit les ressources suivantes pour faciliter la mise en conformité :

- Conformité et gouvernance de la sécurité : ces guides de mise en œuvre de solutions traitent des considérations architecturales et fournissent les étapes à suivre afin de déployer des fonctionnalités de sécurité et de conformité.
- Référence des services éligibles HIPAA : liste les services éligibles HIPAA. Tous ne Services AWS sont pas éligibles à la loi HIPAA.
- AWS Ressources de https://aws.amazon.com/compliance/resources/ de conformité — Cette collection de classeurs et de guides peut s'appliquer à votre secteur d'activité et à votre région.
- 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 en matière de sécurisation Services AWS et décrivent les directives relatives aux contrôles de sécurité dans de nombreux cadres (notamment le National Institute of Standards and Technology (NIST), le Payment Card Industry Security Standards Council (PCI) et l'Organisation internationale de normalisation (ISO)).
- Évaluation des ressources à l'aide des règles du guide du AWS Config développeur : le AWS Config service évalue dans quelle mesure les configurations de vos ressources sont conformes aux pratiques internes, aux directives du secteur et aux réglementations.
- AWS Security Hub— Cela Service AWS fournit une vue complète de votre état de sécurité interne 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 — Cela Service AWS détecte les menaces potentielles qui pèsent sur vos charges de travail Comptes AWS, vos conteneurs et vos données en surveillant votre environnement pour détecter toute activité suspecte et malveillante. GuardDuty peut vous aider à répondre à diverses exigences de conformité, telles que la norme PCI DSS, en répondant aux exigences de détection des intrusions imposées par certains cadres de conformité.

- AWS Audit Manager— Cela vous Service AWS permet d'auditer en permanence votre AWS utilisation afin de 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 est construite autour Régions AWS de zones de disponibilité. Régions AWS fournissent plusieurs zones de disponibilité physiquement séparées et isolées, connectées par un réseau à faible latence, à haut débit et hautement redondant. 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 les zones de disponibilité Régions AWS et les zones de disponibilité, consultez la section Infrastructure AWS globale.

Outre l'infrastructure AWS mondiale, AWS End User Messaging Social propose plusieurs fonctionnalités pour répondre à vos besoins en matière de résilience et de sauvegarde des 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 décrites dans le livre blanc Amazon Web Services : présentation des processus de sécurité.

Vous utilisez des appels d'API AWS publiés pour accéder à AWS End User Messaging Social via le réseau. Les clients doivent supporter le protocole TLS (Sécurité de la couche transport) 1.0 ou une version ultérieure. Nous recommandons TLS 1.2 ou version ultérieure. Les clients doivent aussi prendre en charge les suites de chiffrement PFS (Perfect Forward Secrecy) comme DHE (Ephemeral Diffie-Hellman) ou 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 principal IAM. 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. En AWS, l'usurpation d'identité interservices peut entraîner la confusion des adjoints. 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 député confus consiste à utiliser la clé de contexte de condition globale `aws:SourceArn` avec l'ARN complet de la ressource. Si vous ne connaissez pas l'ARN complet de la ressource ou si vous spécifiez plusieurs ressources, utilisez la clé de contexte de condition globale `aws:SourceArn` avec des caractères génériques (*) pour les parties inconnues de l'ARN. Par exemple, `arn:aws:social-messaging:*:`*`123456789012`*`:*`.

Si la valeur `aws:SourceArn` ne contient pas l'ID du compte, tel qu'un ARN de compartiment Amazon S3, 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 contextuelles `aws:SourceArn` et les clés de contexte de condition `aws:SourceAccount` globale dans la messagerie sociale pour éviter le problème de confusion des adjoints.

```
{
```

```
  "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 un certain nombre de fonctionnalités de sécurité à prendre en compte lors de l'élaboration et de la mise en œuvre de vos propres politiques 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 individuel pour chaque personne qui gère les ressources sociales de messagerie des utilisateurs AWS finaux, y compris vous-même. N'utilisez pas les informations d'identification AWS root pour gérer les ressources sociales de messagerie des utilisateurs AWS finaux.
- Accordez à chaque utilisateur un ensemble minimum d'autorisations requises pour exécuter ses tâches.
- Utilisez des groupes IAM pour gérer efficacement des autorisations pour plusieurs utilisateurs.
- Effectuer une rotation régulière des informations d'identification IAM.

Utilisation de rôles liés à un service pour la messagerie sociale de l'utilisateur AWS final

AWS La messagerie utilisateur final utilise des rôles AWS Identity and Access Management liés au service (IAM). Un rôle lié à un service est un type unique de rôle IAM directement lié à AWS End User Messaging Social. Les rôles liés aux services sont prédéfinis par AWS End User Messaging Social et incluent toutes les autorisations dont le service a besoin pour appeler d'autres AWS services en votre nom.

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

Vous pouvez supprimer un rôle lié à un service uniquement après la suppression préalable de ses ressources connexes. Cela protège vos ressources sociales de messagerie à l'utilisateur AWS final, car vous ne pouvez pas supprimer par inadvertance l'autorisation d'accès à ces ressources.

Pour plus d'informations sur les autres services qui prennent en charge les rôles liés à un service, consultez la section AWS Services qui fonctionnent avec IAM et recherchez les services dont la valeur est Oui dans la colonne Rôles liés à un service. Sélectionnez un Oui ayant un lien pour consulter la documentation du rôle lié à un service, pour ce service.

Autorisations de rôle liées au service pour l'utilisateur AWS final Messaging Social

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 AWSService RoleForSocialMessaging lié à un service fait confiance aux services suivants pour assumer le rôle :

- `social-messaging.amazonaws.com`

La politique d'autorisation des rôles nommée AWSSocial MessagingServiceRolePolicy 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 Autorisations de rôles liés à un service dans le Guide de l'utilisateur IAM.

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 l'utilisateur AWS final Messaging Social

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

Vous pouvez créer le rôle lié à un service pour AWS End User Messaging Social à l'aide de la commande suivante : AWS CLI

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

Modification d'un rôle lié à un service pour AWS End User Messaging Social

AWS End User Messaging Social ne vous permet pas de modifier le rôle AWSService RoleForSocialMessaging lié au 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 d'IAM. Pour plus d'informations, consultez Modification d'un rôle lié à un service dans le IAM Guide de l'utilisateur.

Suppression d'un rôle lié à un service pour AWS End User Messaging Social

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 social 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 AWSService RoleForSocialMessaging

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

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

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

Régions prises en charge pour les AWS rôles liés aux services sociaux de messagerie à l'utilisateur final

AWS Final User Messaging Social prend en charge l'utilisation de rôles liés au service dans toutes les régions où le service est disponible. Pour de plus amples informations, veuillez consulter AWS Régions et points de terminaison.

Accédez à AWS la messagerie sociale de l'utilisateur final à l'aide d'un point de terminaison d'interface (AWS PrivateLink)

Vous pouvez l'utiliser AWS PrivateLink pour créer une connexion privée entre votre VPC et AWS End User Messaging Social. Vous pouvez accéder à AWS End User Messaging Social comme s'il se trouvait dans votre VPC, sans utiliser de passerelle Internet, de périphérique NAT, de connexion VPN ou AWS Direct Connect de connexion. Les instances de votre VPC n'ont pas besoin d'adresses IP publiques pour accéder à AWS End User Messaging Social.

Vous établissez cette connexion privée en créant un point de terminaison d’interface optimisé par AWS PrivateLink. Nous créons une interface réseau de point de terminaison dans chaque sous-réseau que vous activez pour le point de terminaison d’interface. Il s'agit d'interfaces réseau gérées par les demandeurs qui servent de point d'entrée pour le trafic destiné à la messagerie sociale de l'utilisateur AWS final.

Pour plus d'informations, consultez la section Accès Services AWS par AWS PrivateLink le biais du AWS PrivateLink guide.

Considérations relatives à AWS la messagerie sociale destinée aux utilisateurs finaux

Avant de configurer un point de terminaison d'interface pour AWS End User Messaging Social, consultez les considérations du AWS PrivateLink guide.

AWS End User Messaging Social permet d'appeler toutes ses actions d'API via le point de terminaison de l'interface.

Les politiques de point de terminaison VPC ne sont pas prises en charge pour AWS End User Messaging Social. Par défaut, l'accès complet à AWS End User Messaging Social est autorisé via le point de terminaison de l'interface. Vous pouvez également associer un groupe de sécurité aux interfaces réseau du point de terminaison pour contrôler le trafic vers AWS End User Messaging Social via le point de terminaison de l'interface.

Création d'un point de terminaison d'interface pour l'utilisateur AWS final Messaging Social

Vous pouvez créer un point de terminaison d'interface pour AWS End User Messaging Social à l'aide de la console Amazon VPC ou du AWS Command Line Interface ()AWS CLI. Pour plus d'informations, consultez Création d'un point de terminaison d'interface dans le Guide AWS PrivateLink .

Créez un point de terminaison d'interface pour AWS End User Messaging Social en utilisant le nom de service suivant :

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

Si vous activez le DNS privé pour le point de terminaison de l'interface, vous pouvez envoyer des demandes d'API à AWS End User Messaging Social en utilisant son nom DNS régional par défaut. Par exemple, `service-name.us-east-1.amazonaws.com`.

Création d'une politique de point de terminaison pour votre point de terminaison d'interface

Une politique de point de terminaison est une ressource IAM que vous pouvez attacher à votre point de terminaison d'interface. La politique de point de terminaison par défaut autorise un accès complet à AWS End User Messaging Social via le point de terminaison de l'interface. Pour contrôler l'accès autorisé à AWS End User Messaging Social depuis votre VPC, associez une politique de point de terminaison personnalisée au point de terminaison de l'interface.

Une politique de point de terminaison spécifie les informations suivantes :

- Les principaux qui peuvent effectuer des actions (Comptes AWS, utilisateurs IAM et rôles IAM).
- Les actions qui peuvent être effectuées.
- La ressource sur laquelle les actions peuvent être effectuées.

Pour plus d'informations, consultez Contrôle de l'accès aux services à l'aide de politiques de point de terminaison dans le Guide AWS PrivateLink .

Exemple : politique de point de terminaison VPC pour les actions sociales de messagerie de l'utilisateur AWS final

Voici un exemple de politique de point de terminaison personnalisée. Lorsque vous associez cette politique au point de terminaison de votre interface, elle accorde l'accès aux actions sociales de messagerie utilisateur AWS final répertoriées pour tous les principaux sur toutes les ressources.

```
{
   "Statement": [
      {
         "Principal": "*",
         "Effect": "Allow",
         "Action": [
            "social-messaging:DeleteWhatsAppMessageMedia",
            "social-messaging:PostWhatsAppMessageMedia",
            "social-messaging:SendWhatsAppMessage"
         ],
         "Resource":"*"
      }
   ]
}
```

Quotas pour AWS la messagerie sociale destinée aux utilisateurs finaux

Votre compte AWS dispose de quotas par défaut, anciennement appelés limites, pour chaque service AWS. 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.

Votre compte AWS dispose des quotas suivants relatifs à la messagerie sociale destinée aux utilisateurs AWS finaux.

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 envoyer à l'API AWS End User Messaging Social depuis votre Compte AWS.

Opération	Quota de taux par défaut (demandes par seconde)
SendWhatsAppMessage	1 000
PostWhatsAppMessageMedia	100
GetWhatsAppMessageMedia	100
DeleteWhatsAppMessageMedia	100
DisassociateWhatsAppBusinessAccount	10
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 versions de documentation relatives à AWS End User Messaging Social.

Modification	Description	Date
Facturé par message	À compter du 1er juillet 2025, AWS End User Messaging Social facturera par message plutôt que par conversation pour les WhatsApp messages. Pour plus d'informations, consultez la section Facturé par message.	30 juin 2025
Disponibilité par région	Ajout du support pour la région Europe (Francfort). Pour plus d'informations, consultez la section Disponibilité régionale.	5 décembre 2024
Ajouter un message et une destination d'événement	Ajout de la prise en charge d'Amazon Connect en tant que destination d'événements. Pour plus d'informations, voir Ajouter un message et une destination d'événement.	1er décembre 2024
AWS PrivateLink	Ajout du support pour AWS PrivateLink. Pour de plus amples informations, veuillez consulter AWS PrivateLink.	22 octobre 2024
Première version	Publication initiale du Guide de l'utilisateur social de la	10 octobre 2024

messagerie pour utilisateurs AWS finaux

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.