aws

Guide d’administration

Wickr AWS

Wickr AWS: Guide d’administration

Table of Contents

Qu'est-ce qu'AWS Wickr ?

AWS Wickr est un service end-to-end crypté qui aide les organisations et les agences gouvernementales à communiquer en toute sécurité par le biais one-to-one de la messagerie de groupe, des appels vocaux et vidéo, du partage de fichiers, du partage d'écran, etc. Wickr peut aider les clients à surmonter les obligations de conservation des données associées aux applications de messagerie grand public et à faciliter la collaboration en toute sécurité. Les contrôles de sécurité et administratifs avancés aident les entreprises à répondre aux exigences légales et réglementaires et à créer des solutions personnalisées pour relever les défis liés à la sécurité des données.

Les informations peuvent être enregistrées dans un magasin de données privé contrôlé par le client à des fins de conservation et d'audit. Les utilisateurs disposent d'un contrôle administratif complet sur les données, notamment en définissant des autorisations, en configurant des options de messagerie éphémère et en définissant des groupes de sécurité. Wickr s'intègre à des services supplémentaires tels qu'Active Directory (AD), l'authentification unique (SSO) avec OpenID Connect (OIDC), etc. Vous pouvez créer et gérer rapidement un réseau Wickr via les AWS Management Console robots Wickr et automatiser en toute sécurité les flux de travail. Consultez Configuration d'AWS Wickr pour démarrer.

Rubriques

Caractéristiques de Wickr

Sécurité et confidentialité renforcées

Wickr utilise un cryptage AES (Advanced Encryption Standard) end-to-end 256 bits pour chaque fonctionnalité. Les communications sont cryptées localement sur les appareils des utilisateurs et restent indéchiffrables en transit pour toute personne autre que l'expéditeur et le destinataire. Chaque message, appel et fichier est chiffré avec une nouvelle clé aléatoire, et personne d'autre que les destinataires prévus (même pas AWS) ne peut les déchiffrer. Qu'il s'agisse de partager des données sensibles et réglementées, de discuter de questions juridiques ou RH, ou même de mener des

opérations militaires tactiques, les clients utilisent Wickr pour communiquer lorsque la sécurité et la confidentialité sont primordiales.

Conservation des données

Les fonctionnalités administratives flexibles sont conçues non seulement pour protéger les informations sensibles, mais aussi pour conserver les données conformément aux obligations de conformité, à la conservation légale et à des fins d'audit. Les messages et les fichiers peuvent être archivés dans un magasin de données sécurisé contrôlé par le client.

Accès flexible

Les utilisateurs disposent d'un accès à plusieurs appareils (mobile, ordinateur de bureau) et peuvent fonctionner dans des environnements à faible bande passante, notamment en cas de déconnexion et out-of-band de communication.

Contrôles administratifs

Les utilisateurs disposent d'un contrôle administratif complet sur les données, notamment en définissant des autorisations, en configurant des options de messagerie éphémère responsables et en définissant des groupes de sécurité.

Intégrations et robots puissants

Wickr s'intègre à des services supplémentaires tels qu'Active Directory, l'authentification unique (SSO) avec OpenID Connect (OIDC), etc. Les clients peuvent créer et gérer rapidement un réseau Wickr grâce à Wickr AWS Management Console Bots et automatiser en toute sécurité les flux de travail.

Voici un aperçu des offres de collaboration de Wickr :

- Messagerie individuelle et de groupe : discutez en toute sécurité avec votre équipe dans les salles comptant jusqu'à 500 membres
- Appels audio et vidéo : organisez des conférences téléphoniques avec un maximum de 70 personnes
- Partage d'écran et diffusion : présentez devant un maximum de 500 participants
- Partage et sauvegarde de fichiers : transférez jusqu'à 5 fichiers GBs avec un stockage illimité
- Éphémère : contrôlez l'expiration et les délais burn-on-read
- Fédération mondiale : connectez-vous aux utilisateurs de Wickr en dehors de votre réseau

Disponibilité par région

Wickr est disponible dans l'est des États-Unis (Virginie du Nord), en Asie-Pacifique (Malaisie), en Asie-Pacifique (Singapour), en Asie-Pacifique (Sydney), en Asie-Pacifique (Tokyo), au Canada (centre), en Europe (Francfort), en Europe (Londres), en Europe (Stockholm) et en Europe (Zurich). Régions AWS Wickr est également disponible dans la région AWS GovCloud (ouest des États-Unis). Chaque région contient plusieurs zones de disponibilité, qui sont physiquement séparées mais connectées par des connexions réseau privées, à faible latence, à bande passante élevée et redondantes. Ces zones de disponibilité sont utilisées pour améliorer la disponibilité, la tolérance aux pannes et la latence minimisée.

Pour en savoir plus Régions AWS, consultez Spécifiez ce que Régions AWS votre compte peut utiliser dans le Références générales AWS. Pour plus d'informations sur le nombre de zones de disponibilité disponibles dans chaque région, consultez la section Infrastructure AWS mondiale.

Accès à Wickr

Les administrateurs accèdent au AWS Management Console for Wickr à l'adresse https://console.aws.amazon.com/wickr/. Avant de commencer à utiliser Wickr, vous devez suivre les Commencer à utiliser AWS Wickr guides Configuration d'AWS Wickr et.

Les utilisateurs finaux accèdent à Wickr via le client Wickr. Pour plus d'informations, consultez le guide de l'utilisateur d'AWS Wickr.

Tarification

Wickr est disponible en différents forfaits pour les particuliers, les petites équipes et les grandes entreprises. Pour plus d'informations, consultez la section Tarification d'AWS Wickr.

Documentation pour l'utilisateur final de Wickr

Si vous êtes un utilisateur final du client Wickr et que vous devez accéder à sa documentation, consultez le guide de l'utilisateur d'AWS Wickr.

Configuration d'AWS Wickr

Si vous êtes un nouveau AWS client, remplissez les conditions de configuration requises répertoriées sur cette page avant de commencer à utiliser AWS Wickr. Pour ces procédures de configuration, vous utilisez le service Gestion des identités et des accès AWS (IAM). Pour des informations complètes sur IAM, consultez le Guide de l'utilisateur IAM.

Rubriques

Inscrivez-vous pour 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.

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

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

Créer un utilisateur IAM

Afin de créer un utilisateur administrateur, choisissez l'une des options suivantes :

Choisissez un moyen de gérer votre administrateur	À	En	Vous pouvez également
Dans IAM Identity Center (Recommandé)	Utiliser des informations d'identification à court terme pour accéder à AWS. C'est conforme aux bonnes pratiques en matière de sécurité. Pour plus d'informations sur les bonnes pratiques, consultez Bonnes pratiques de sécurité dans IAM dans le Guide de l'utilisateur IAM.	Suivant les instructions fournies dans Mise en route dans le Guide de l'utilisateur AWS IAM Identity Center .	Configurez l'accès par programmation en configurant le AWS CLI à utiliser AWS IAM Identity Center dans le guide de l'AWS Command Line Interface utilisateur.
Dans IAM (Non recommandé)	Utiliser des identifiants à long terme pour accéder à AWS.	Suivre les instructions relatives à la Création de votre premier groupe utilisateur administrateur et utilisateur IAM dans le Guide de l'utilisateur IAM.	Configuration de l'accès par programmation via la Gestion des clés d'accès pour les utilisateurs IAM dans le Guide de l'utilisateur IAM.

> **Note**
>
> Vous pouvez également attribuer la politique `AWSWickrFullAccess` gérée pour accorder une autorisation administrative complète au service Wickr. Pour de plus amples informations, veuillez consulter AWS politique gérée : AWSWickr FullAccess.

Quelle est la prochaine étape

Vous avez effectué les étapes de configuration préalables. Pour commencer à configurer Wickr, consultezPrise en main.

Commencer à utiliser AWS Wickr

Dans ce guide, nous vous montrons comment démarrer avec Wickr en créant un réseau, en configurant votre réseau et en créant des utilisateurs.

Rubriques

Conditions préalables

Avant de commencer, assurez-vous de remplir les conditions préalables suivantes si ce n'est déjà fait :

- Inscrivez-vous à Amazon Web Services (AWS). Pour de plus amples informations, veuillez consulter Configuration d'AWS Wickr.
- Assurez-vous de disposer des autorisations requises pour administrer Wickr. Pour de plus amples informations, veuillez consulter AWS politique gérée : AWSWickr FullAccess.
- Assurez-vous d'autoriser la liste des ports et domaines appropriés pour Wickr. Pour de plus amples informations, veuillez consulter Liste des ports et domaines à autoriser pour votre réseau Wickr.

Étape 1 : créer un réseau

Vous pouvez créer un réseau Wickr.

Suivez la procédure suivante pour créer un réseau Wickr pour votre compte.

1. Ouvrez le AWS Management Console pour Wickr à l'adresse https://console.aws.amazon.com/wickr/.

   > **Note**
   >
   > Si vous n'avez jamais créé de réseau Wickr auparavant, vous verrez la page d'information du service Wickr. Après avoir créé un ou plusieurs réseaux Wickr, vous

verrez la page Réseaux, qui contient une liste de tous les réseaux Wickr que vous avez créés.

2. Choisissez Créer un réseau.
3. Entrez le nom de votre réseau dans la zone de texte Nom du réseau. Choisissez un nom que les membres de votre organisation reconnaîtront, tel que le nom de votre entreprise ou le nom de votre équipe.
4. Choisissez un plan. Vous pouvez choisir l'un des plans de réseau Wickr suivants :

   - Standard — Pour les équipes des petites et grandes entreprises qui ont besoin de contrôles administratifs et de flexibilité.
   - Essai gratuit Premium ou Premium : pour les entreprises qui ont besoin des limites de fonctionnalités les plus élevées, de contrôles administratifs précis et de la conservation des données.

   Les administrateurs ont la possibilité de sélectionner un essai gratuit premium, disponible pour un maximum de 30 utilisateurs et d'une durée de trois mois. En AWS WickrGov effet, l'option d'essai gratuit premium permet jusqu'à 50 utilisateurs et dure également trois mois. Pendant la période d'essai gratuite Premium, les administrateurs peuvent passer à un forfait Premium ou Standard ou à un forfait inférieur.

   Pour plus d'informations sur les forfaits et les tarifs Wickr disponibles, consultez la page de tarification Wickr.
5. (Facultatif) Choisissez Ajouter un nouveau tag pour ajouter un tag à votre réseau. Les balises sont constituées d'une paire clé-valeur. Les tags peuvent être utilisés pour rechercher et filtrer les ressources ou pour suivre vos AWS coûts. Pour plus d'informations, consultez la section Balises réseau.
6. Choisissez Create Network.

   Vous êtes redirigé vers la page Réseaux de AWS Management Console for Wickr, et le nouveau réseau est répertorié sur la page.

Étape 2 : Configuration de votre réseau

Suivez la procédure suivante AWS Management Console pour accéder à Wickr, où vous pouvez ajouter des utilisateurs, ajouter des groupes de sécurité, configurer le SSO, configurer la conservation des données et des paramètres réseau supplémentaires.

1. Sur la page Réseaux, sélectionnez le nom du réseau pour accéder à ce réseau.

   Vous êtes redirigé vers la console d'administration Wickr pour le réseau sélectionné.

2. Les options de gestion des utilisateurs suivantes sont disponibles. Pour plus d'informations sur la configuration de ces paramètres, consultez Gérez votre réseau AWS Wickr.

   - Groupe de sécurité : gérez les groupes de sécurité et leurs paramètres, tels que les politiques de complexité des mots de passe, les préférences de messagerie, les fonctionnalités d'appel, les fonctionnalités de sécurité et la fédération externe. Pour de plus amples informations, veuillez consulter Groupes de sécurité pour AWS Wickr.
   - Configuration de l'authentification unique (SSO) — Configurez l'authentification unique et affichez l'adresse du point de terminaison de votre réseau Wickr. Wickr prend en charge les fournisseurs SSO qui utilisent uniquement OpenID Connect (OIDC). Les fournisseurs qui utilisent le langage SAML (Security Assertion Markup Language) ne sont pas pris en charge. Pour de plus amples informations, veuillez consulter Configuration de l'authentification unique pour AWS Wickr.

Étape 3 : créer et inviter des utilisateurs

Vous pouvez créer des utilisateurs dans votre réseau Wickr en utilisant les méthodes suivantes :

- Authentification unique — Si vous configurez l'authentification unique, vous pouvez inviter des utilisateurs en partageant votre identifiant d'entreprise Wickr. Les utilisateurs finaux s'inscrivent à Wickr en utilisant l'identifiant d'entreprise fourni et leur adresse e-mail professionnelle. Pour de plus amples informations, veuillez consulter Configuration de l'authentification unique pour AWS Wickr.
- Invitation — Vous pouvez créer manuellement des utilisateurs dans le AWS Management Console for Wickr et leur faire envoyer une invitation par e-mail. Les utilisateurs finaux peuvent s'inscrire à Wickr en cliquant sur le lien contenu dans l'e-mail.

> **Note**
>
> Vous pouvez également activer les utilisateurs invités pour votre réseau Wickr. Pour de plus amples informations, consultez Utilisateurs invités du réseau AWS Wickr.

Suivez les procédures ci-dessous pour créer ou inviter des utilisateurs.

> **Note**
>
> Les administrateurs sont également considérés comme des utilisateurs et doivent s'inviter sur les réseaux Wickr SSO ou non SSO.

Pour créer des utilisateurs Wickr et envoyer des invitations par SSO :

Écrivez et envoyez un e-mail aux utilisateurs du SSO qui doivent s'inscrire à Wickr. Incluez les informations suivantes dans votre e-mail :

- Votre identifiant d'entreprise Wickr. Vous spécifiez un identifiant d'entreprise pour votre réseau Wickr lorsque vous configurez le SSO. Pour de plus amples informations, veuillez consulter Configuration de l'authentification unique dans AWS Wickr.
- L'adresse e-mail qu'ils doivent utiliser pour s'inscrire.
- URL permettant de télécharger le client Wickr. Les utilisateurs peuvent télécharger les clients Wickr depuis la page de téléchargement d'AWS Wickr à https://aws.amazon.com/wickr/ l'adresse download/.

  > **Note**
  >
  > Si vous avez créé votre réseau Wickr dans AWS GovCloud l'ouest des États-Unis, demandez à vos utilisateurs de télécharger et d'installer le client. WickrGov Pour toutes les autres AWS régions, demandez à vos utilisateurs de télécharger et d'installer le client Wickr standard. Pour plus d'informations AWS WickrGov, consultez AWS WickrGovle guide de l'AWS GovCloud (US) utilisateur.

Lorsque les utilisateurs s'inscrivent sur votre réseau Wickr, ils sont ajoutés au répertoire de l'équipe Wickr avec le statut actif.

Pour créer manuellement des utilisateurs Wickr et envoyer des invitations :

1. Ouvrez le AWS Management Console pour Wickr à l'adresse https://console.aws.amazon.com/wickr/.
2. Sur la page Réseaux, sélectionnez le nom du réseau pour accéder à ce réseau.

   Vous êtes redirigé vers le réseau Wickr. Dans le réseau Wickr, vous pouvez ajouter des utilisateurs, ajouter des groupes de sécurité, configurer le SSO, configurer la conservation des données et ajuster des paramètres supplémentaires.
3. Dans le volet de navigation, sélectionnez Gestion des utilisateurs.
4. Sur la page Gestion des utilisateurs, sous l'onglet Annuaire de l'équipe, choisissez Inviter un utilisateur.

   Vous pouvez également inviter des utilisateurs en bloc en cliquant sur la flèche déroulante située à côté de Inviter un utilisateur. Sur la page Inviter des utilisateurs par lots, sélectionnez Télécharger le modèle pour télécharger un modèle CSV que vous pouvez modifier et charger avec votre liste d'utilisateurs.
5. Entrez le prénom, le nom de famille, le code du pays, le numéro de téléphone et l'adresse e-mail de l'utilisateur. L'adresse e-mail est le seul champ obligatoire. Assurez-vous de choisir le groupe de sécurité approprié pour l'utilisateur.
6. Choisissez Inviter.

   Wickr envoie un e-mail d'invitation à l'adresse que vous spécifiez pour l'utilisateur. L'e-mail fournit des liens de téléchargement pour les applications clientes Wickr, ainsi qu'un lien pour s'inscrire à Wickr. Pour plus d'informations sur ce à quoi ressemble cette expérience utilisateur final, consultez Télécharger l'application Wickr et accepter votre invitation dans le guide de l'utilisateur d'AWS Wickr.

   Lorsque les utilisateurs s'inscrivent à Wickr en utilisant le lien contenu dans l'e-mail, leur statut dans le répertoire de l'équipe Wickr passe de En attente à Actif.

Étapes suivantes

Vous avez terminé les étapes de démarrage. Pour gérer Wickr, consultez ce qui suit :

- Gérez votre réseau AWS Wickr

- Gérer les utilisateurs dans AWS Wickr

Gérez votre réseau AWS Wickr

Dans AWS Management Console for Wickr, vous pouvez gérer le nom de votre réseau Wickr, les groupes de sécurité, la configuration SSO et les paramètres de conservation des données.

Rubriques

Détails du réseau pour AWS Wickr

Vous pouvez modifier le nom de votre réseau Wickr et consulter votre identifiant réseau dans la section Détails du réseau du AWS Management Console pour Wickr.

Rubriques

Afficher les détails du réseau dans AWS Wickr

Vous pouvez consulter les détails de votre réseau Wickr, y compris le nom et l'identifiant de votre réseau.

Suivez la procédure suivante pour afficher votre profil réseau Wickr et votre identifiant réseau.

1. Ouvrez le AWS Management Console pour Wickr à l'adresse https://console.aws.amazon.com/wickr/.
2. Sur la page Réseaux, recherchez le réseau que vous souhaitez consulter.
3. Sur le côté droit du réseau que vous souhaitez afficher, sélectionnez l'icône représentant des points de suspension verticaux (trois points), puis choisissez Afficher les détails.

   La page d'accueil du réseau affiche le nom et l'identifiant de votre réseau Wickr dans la section Détails du réseau. Vous pouvez utiliser l'ID réseau pour configurer la fédération.

Modifier le nom du réseau dans AWS Wickr

Vous pouvez modifier le nom de votre réseau Wickr.

Suivez la procédure suivante pour modifier le nom de votre réseau Wickr.

1. Ouvrez le AWS Management Console pour Wickr à l'adresse https://console.aws.amazon.com/wickr/.
2. Sur la page Réseaux, sélectionnez le nom du réseau pour accéder à la console d'administration Wickr correspondant à ce réseau.
3. Sur la page d'accueil du réseau, dans la section Détails du réseau, choisissez Modifier.
4. Entrez le nouveau nom de votre réseau dans la zone de texte Nom du réseau.
5. Choisissez Enregistrer pour enregistrer le nouveau nom de votre réseau.

Supprimer le réseau dans AWS Wickr

Vous pouvez supprimer votre réseau AWS Wickr.

> **Note**
>
> Si vous supprimez un réseau d'essai gratuit premium, vous ne pourrez pas en créer un autre.

Pour supprimer votre réseau Wickr sur la page d'accueil des réseaux, procédez comme suit.

1. Ouvrez le AWS Management Console pour Wickr à l'adresse https://console.aws.amazon.com/wickr/.

2. Sur la page Réseaux, recherchez le réseau que vous souhaitez supprimer.
3. Sur le côté droit du réseau que vous souhaitez supprimer, sélectionnez l'icône représentant des points de suspension verticaux (trois points), puis choisissez Supprimer le réseau.
4. Tapez Confirmer dans la fenêtre contextuelle, puis choisissez Supprimer.

   La suppression du réseau peut prendre quelques minutes.

Pour supprimer votre réseau Wickr alors qu'il est sur le réseau, procédez comme suit.

1. Ouvrez le AWS Management Console pour Wickr à l'adresse https://console.aws.amazon.com/wickr/.
2. Sur la page Réseaux, sélectionnez le réseau que vous souhaitez supprimer.
3. Dans le coin supérieur droit de la page d'accueil du réseau, choisissez Supprimer le réseau.
4. Tapez Confirmer dans la fenêtre contextuelle, puis choisissez Supprimer.

   La suppression du réseau peut prendre quelques minutes.

> **Note**
>
> Les données conservées par votre configuration de conservation des données (si elle est activée) ne seront pas supprimées lorsque vous supprimerez votre réseau. Pour plus d'informations, consultez la section Conservation des données pour AWS Wickr.

Groupes de sécurité pour AWS Wickr

Dans la section Groupes de sécurité de AWS Management Console for Wickr, vous pouvez gérer les groupes de sécurité et leurs paramètres, tels que les politiques de complexité des mots de passe, les préférences de messagerie, les fonctionnalités d'appel, les fonctionnalités de sécurité et la fédération réseau.

Rubriques

Afficher les groupes de sécurité dans AWS Wickr

Vous pouvez consulter les détails de vos groupes de sécurité Wickr.

Suivez la procédure ci-dessous pour afficher les groupes de sécurité.

1. Ouvrez le AWS Management Console pour Wickr à l'adresse https://console.aws.amazon.com/wickr/.
2. Sur la page Réseaux, sélectionnez le nom du réseau pour accéder à ce réseau.
3. Dans le panneau de navigation, choisissez Groupes de sécurité.

   La page Groupes de sécurité affiche vos groupes de sécurité Wickr actuels et vous donne la possibilité de créer un nouveau groupe.

   Sur la page Groupes de sécurité, sélectionnez le groupe de sécurité que vous souhaitez afficher. La page affichera les détails actuels de ce groupe de sécurité.

Création d'un groupe de sécurité dans AWS Wickr

Vous pouvez créer un nouveau groupe de sécurité Wickr.

Suivez la procédure ci-dessous pour créer un groupe de sécurité.

1. Ouvrez le AWS Management Console pour Wickr à l'adresse https://console.aws.amazon.com/wickr/.
2. Sur la page Réseaux, sélectionnez le nom du réseau pour accéder à ce réseau.
3. Dans le panneau de navigation, choisissez Groupes de sécurité.
4. Sur la page Groupes de sécurité, choisissez Créer un groupe de sécurité pour créer un nouveau groupe de sécurité.

   > **Note**
   >
   > Un nouveau groupe de sécurité portant un nom par défaut est automatiquement ajouté à la liste des groupes de sécurité.

5. Sur la page Créer un groupe de sécurité, entrez le nom de votre groupe de sécurité.
6. Sélectionnez Create security group (Créer un groupe de sécurité).

Pour plus d'informations sur la modification du nouveau groupe de sécurité, consultezModifier un groupe de sécurité dans AWS Wickr.

Modifier un groupe de sécurité dans AWS Wickr

Vous pouvez modifier les détails de votre groupe de sécurité Wickr.

Suivez la procédure ci-dessous pour modifier un groupe de sécurité.

1. Ouvrez le AWS Management Console pour Wickr à l'adresse https://console.aws.amazon.com/wickr/.
2. Sur la page Réseaux, sélectionnez le nom du réseau pour accéder à ce réseau.
3. Dans le panneau de navigation, choisissez Groupes de sécurité.
4. Sélectionnez le nom du groupe de sécurité que vous souhaitez modifier.

   La page des détails du groupe de sécurité affiche les paramètres du groupe de sécurité dans différents onglets.
5. Les onglets suivants et les paramètres correspondants sont disponibles :

   - Détails du groupe de sécurité — Choisissez Modifier dans la section Détails du groupe de sécurité pour modifier le nom.
   - Messagerie — Gérez les fonctionnalités de messagerie pour les membres du groupe.
     - B urn-on-read — Contrôle la valeur maximale que les utilisateurs peuvent définir pour leurs burn-on-read minuteries dans leurs clients Wickr. Pour plus d'informations, voir Définir les délais d'expiration et de gravure des messages dans le client Wickr.
     - Délai d'expiration — Contrôle la valeur maximale que les utilisateurs peuvent définir pour le délai d'expiration de leurs messages dans leurs clients Wickr. Pour plus d'informations, voir Définir les délais d'expiration et de gravure des messages dans le client Wickr.
     - Transfert de messages — Contrôle si les utilisateurs peuvent transférer des messages dans leurs clients Wickr. Pour plus d'informations, consultez Transférer des messages dans le client Wickr.
     - Réponses rapides — Définissez une liste de réponses rapides permettant aux utilisateurs de répondre aux messages.

- Intensité du destructeur sécurisé — Configurez la fréquence à laquelle le contrôle du destructeur sécurisé s'exécute pour les utilisateurs. Pour plus d'informations, consultez la section Messagerie.

- Appels — Gérez les fonctionnalités d'appel pour les membres du groupe.
  - Activer les appels audio : les utilisateurs peuvent lancer des appels audio.
  - Activer les appels vidéo et le partage d'écran : les utilisateurs peuvent démarrer des appels vidéo ou partager l'écran pendant l'appel.
  - Appels TCP — L'activation (ou le forçage) des appels TCP est généralement utilisée lorsque les ports VoIP UDP standard sont interdits par le service informatique ou de sécurité d'une entreprise. Si les appels TCP sont désactivés et que les ports UDP ne sont pas disponibles, les clients Wickr essaieront d'abord le protocole UDP et reviendront au protocole TCP.
- Médias et liens : gérez les paramètres relatifs aux médias et aux liens pour les membres du groupe.

  Taille de téléchargement du fichier — Sélectionnez la meilleure qualité de transfert pour permettre aux utilisateurs de transférer les fichiers et les pièces jointes sous leur forme cryptée d'origine. Si vous sélectionnez Transfert à faible bande passante, les pièces jointes envoyées par les utilisateurs dans Wickr seront compressées par le service de transfert de fichiers Wickr.
- Localisation — Gérez les paramètres de partage de position pour les membres du groupe.

  Partage de position — Les utilisateurs peuvent partager leur position à l'aide d'appareils compatibles GPS. Cette fonctionnalité affiche une carte visuelle basée sur les paramètres par défaut du système d'exploitation de l'appareil. Les utilisateurs ont la possibilité de désactiver la vue cartographique et de partager un lien contenant leurs coordonnées GPS à la place.
- Sécurité — Configurez des fonctionnalités de sécurité supplémentaires pour le groupe.
  - Activez la protection contre le piratage de compte : appliquez une authentification à deux facteurs lorsqu'un utilisateur ajoute un nouvel appareil à son compte. Pour vérifier un nouvel appareil, l'utilisateur peut générer un code Wickr à partir de son ancien appareil ou effectuer une vérification par e-mail. Il s'agit d'un niveau de sécurité supplémentaire destiné à empêcher tout accès non autorisé aux comptes AWS Wickr.
  - Activer toujours la réauthentification : obligez les utilisateurs à toujours s'authentifier de nouveau lorsqu'ils accèdent à nouveau à l'application.
  - Clé de récupération principale — Crée une clé de récupération principale lors de la création d'un compte. Les utilisateurs peuvent approuver l'ajout d'un nouvel appareil à leur compte si aucun autre appareil n'est disponible.

- Notification et visibilité : configurez les paramètres de notification et de visibilité tels que les aperçus des messages dans les notifications destinées aux membres du groupe.
- Accès ouvert Wickr — Configurez les paramètres de libre accès de Wickr pour les membres du groupe.
  - Activer le libre accès à Wickr — L'activation du libre accès à Wickr masquera le trafic afin de protéger les données sur les réseaux restreints et surveillés. En fonction de la situation géographique, Wickr Open Access se connectera à divers serveurs proxy mondiaux qui fournissent le meilleur chemin et les meilleurs protocoles pour l'obfuscation du trafic.
  - Forcer l'accès ouvert à Wickr — Active et applique automatiquement le libre accès à Wickr sur tous les appareils.
- Fédération — Contrôlez la capacité de vos utilisateurs à communiquer avec d'autres réseaux Wickr.
  - Fédération locale : possibilité de fédérer des AWS utilisateurs d'autres réseaux au sein de la même région. Par exemple, s'il existe deux réseaux dans la région AWS du Canada (Centre) où la fédération locale est activée, ils pourront communiquer entre eux.
  - Fédération mondiale — Possibilité de fédérer soit avec des utilisateurs de Wickr Enterprise, soit avec des AWS utilisateurs d'un réseau différent appartenant à d'autres régions. Par exemple, un utilisateur d'un réseau Wickr dans la région AWS du Canada (Centre) et un utilisateur d'un réseau de la région AWS Europe (Londres) pourront communiquer entre eux lorsque la fédération mondiale est activée pour les deux réseaux.
  - Fédération restreinte : autorise la liste des réseaux AWS Wickr ou Wickr Enterprise spécifiques avec lesquels les utilisateurs peuvent se fédérer. Une fois configuré, les utilisateurs ne peuvent communiquer qu'avec des utilisateurs externes sur les réseaux autorisés. Les deux réseaux doivent s'autoriser à s'inscrire mutuellement pour utiliser la fédération restreinte.

    Pour plus d'informations sur la fédération d'invités, consultez Activer ou désactiver les utilisateurs invités dans le réseau AWS Wickr.
- Configuration du plugin ATAK — Pour plus d'informations sur l'activation d'ATAK, voir Qu'est-ce qu'ATAK ? .

6. Choisissez Enregistrer pour enregistrer les modifications que vous apportez aux détails du groupe de sécurité.

Supprimer un groupe de sécurité dans AWS Wickr

Vous pouvez supprimer votre groupe de sécurité Wickr.

Suivez la procédure ci-dessous pour supprimer un groupe de sécurité.

1. Ouvrez le AWS Management Console pour Wickr à l'adresse https://console.aws.amazon.com/wickr/.
2. Sur la page Réseaux, sélectionnez le nom du réseau pour accéder à ce réseau.
3. Dans le panneau de navigation, choisissez Groupes de sécurité.
4. Sur la page Groupes de sécurité, recherchez le groupe de sécurité que vous souhaitez supprimer.
5. Sur le côté droit du groupe de sécurité que vous souhaitez supprimer, sélectionnez l'icône représentant des points de suspension verticaux (trois points), puis choisissez Supprimer.
6. Tapez Confirmer dans la fenêtre contextuelle, puis choisissez Supprimer.

   Lorsque vous supprimez un groupe de sécurité auquel des utilisateurs ont été affectés, ceux-ci sont automatiquement ajoutés au groupe de sécurité par défaut. Pour modifier le groupe de sécurité attribué aux utilisateurs, voirModifier les utilisateurs dans le réseau AWS Wickr.

Configuration de l'authentification unique pour AWS Wickr

Dans AWS Management Console for Wickr, vous pouvez configurer Wickr pour qu'il utilise un système d'authentification unique pour s'authentifier. Le SSO fournit une couche de sécurité supplémentaire lorsqu'il est associé à un système d'authentification multifactorielle (MFA) approprié. Wickr prend en charge les fournisseurs SSO qui utilisent uniquement OpenID Connect (OIDC). Les fournisseurs qui utilisent le langage SAML (Security Assertion Markup Language) ne sont pas pris en charge.

Rubriques

- Afficher les détails du SSO dans AWS Wickr
- Configuration de l'authentification unique dans AWS Wickr
- Période de grâce pour l'actualisation des jetons

Afficher les détails du SSO dans AWS Wickr

Vous pouvez consulter les détails de votre configuration d'authentification unique pour votre réseau Wickr et le point de terminaison du réseau.

Effectuez la procédure suivante pour afficher la configuration d'authentification unique actuelle pour votre réseau Wickr, le cas échéant.

1. Ouvrez le AWS Management Console pour Wickr à l'adresse https://console.aws.amazon.com/wickr/.
2. Sur la page Réseaux, sélectionnez le nom du réseau pour accéder à ce réseau.
3. Dans le volet de navigation, sélectionnez Gestion des utilisateurs.

   Sur la page Gestion des utilisateurs, la section Single Sign-On affiche le point de terminaison de votre réseau Wickr et la configuration SSO actuelle.

Configuration de l'authentification unique dans AWS Wickr

Pour garantir un accès sécurisé à votre réseau Wickr, vous pouvez configurer votre configuration d'authentification unique actuelle. Des guides détaillés sont disponibles pour vous aider dans ce processus.

⚠ Important

- Lorsque vous configurez le SSO, vous spécifiez un identifiant d'entreprise pour votre réseau Wickr. N'oubliez pas d'enregistrer cet identifiant d'entreprise. Vous devez le fournir à vos utilisateurs finaux lors de l'envoi d'e-mails d'invitation. Les utilisateurs finaux doivent spécifier l'identifiant de l'entreprise lorsqu'ils s'inscrivent à votre réseau Wickr.
- En septembre 2025, AWS Wickr a introduit un système de connexion SSO amélioré et plus sécurisé. Pour tirer parti de ces améliorations de sécurité, les organisations utilisant le SSO doivent migrer vers une nouvelle URI de redirection avant le 9 mars 2026. Pour obtenir des instructions de migration, consultez l' AWS re:Post article suivant : Migration vers la nouvelle URI de redirection SSO pour AWS Wickr.

Pour plus d'informations sur la configuration de l'authentification unique, consultez les guides suivants :

- Configuration de l'authentification unique (SSO) AWS Wickr avec Microsoft Entra (Azure AD)
- Configuration de l'authentification unique (SSO) AWS Wickr avec Okta
- Configuration de l'authentification unique (SSO) AWS Wickr avec Amazon Cognito

Configurer AWS Wickr avec l'authentification unique Microsoft Entra (Azure AD)

AWS Wickr peut être configuré pour utiliser Microsoft Entra (Azure AD) en tant que fournisseur d'identité. Pour ce faire, suivez les procédures suivantes dans Microsoft Entra et dans la console d'administration AWS Wickr.

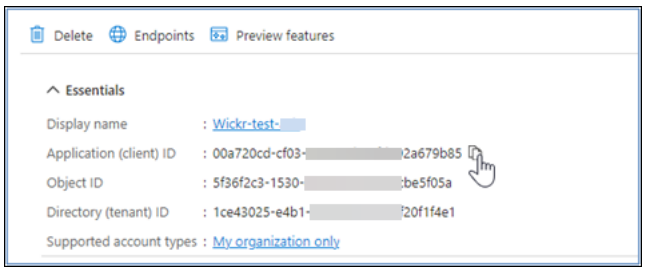
> **Warning**
>
> Une fois le SSO activé sur un réseau, les utilisateurs actifs seront déconnectés de Wickr et les obligeront à s'authentifier à nouveau à l'aide du fournisseur SSO.

Étape 1 : enregistrer AWS Wickr en tant qu'application dans Microsoft Entra

Suivez la procédure suivante pour enregistrer AWS Wickr en tant qu'application dans Microsoft Entra.

> **Note**
>
> Reportez-vous à la documentation Microsoft Entra pour obtenir des captures d'écran détaillées et un dépannage. Pour plus d'informations, voir Enregistrer une application auprès de la plateforme d'identité Microsoft

1. Dans le volet de navigation, choisissez Applications, puis cliquez sur Inscriptions d'applications.
2. Sur la page Inscriptions d'applications, choisissez Enregistrer une application, puis entrez le nom de l'application.
3. Sélectionnez Comptes uniquement dans ce répertoire d'organisation (répertoire par défaut uniquement - Locataire unique).
4. Sous URI de redirection, sélectionnez Web, puis entrez l'URI de redirection disponible dans les paramètres de configuration SSO de la console d'administration AWS Wickr
5. Choisissez S'inscrire.
6. Après l'enregistrement, copy/save l'identifiant de l'application (client) est généré.



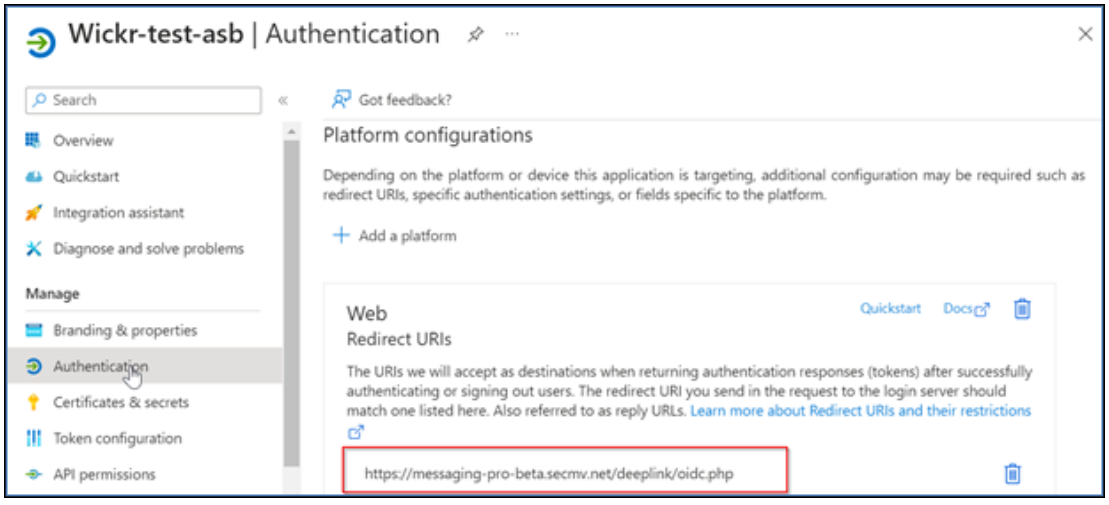
7. Sélectionnez l'onglet Endpoints pour prendre note des points suivants :

    1. Point de terminaison d'autorisation Oauth 2.0 (v2) : Par exemple : `https://login.microsoftonline.com/1ce43025-e4b1-462d-a39f-337f20f1f4e1/oauth2/v2.0/authorize`
    2. Modifiez cette valeur pour supprimer « oauth2/ » et « authorize ». Par exemple, l'URL fixe ressemblera à ceci : `https://login.microsoftonline.com/1ce43025-e4b1-462d-a39f-337f20f1f4e1/v2.0/`
    3. Il sera référencé en tant qu'émetteur SSO.

Étape 2 : Configuration de l'authentification

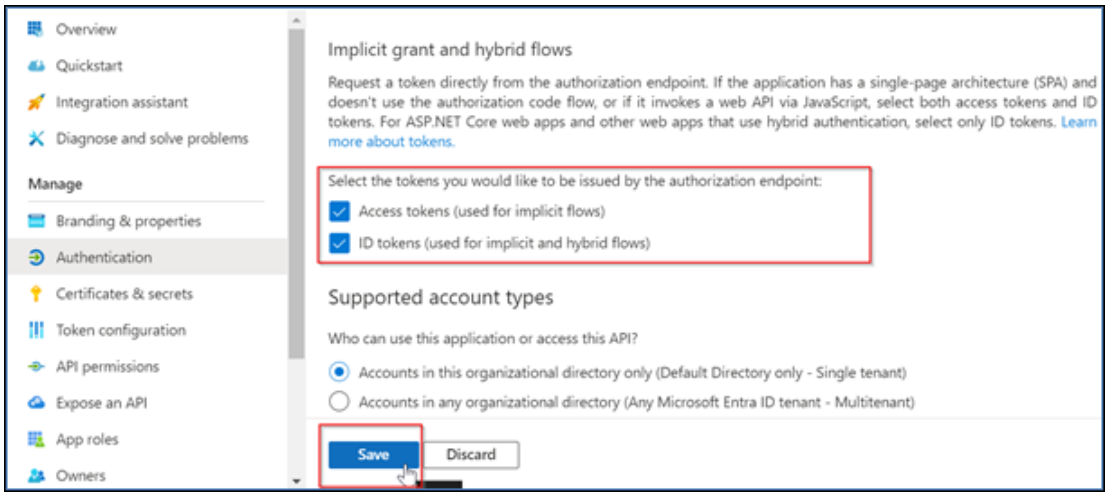
Suivez la procédure ci-dessous pour configurer l'authentification dans Microsoft Entra.

1. Dans le volet de navigation, choisissez Authentication.
2. Sur la page d'authentification, assurez-vous que l'URI de redirection Web est le même que celui saisi précédemment (dans Enregistrer AWS Wickr en tant qu'application).



3. Sélectionnez les jetons d'accès utilisés pour les flux implicites et les jetons d'identification utilisés pour les flux implicites et hybrides.

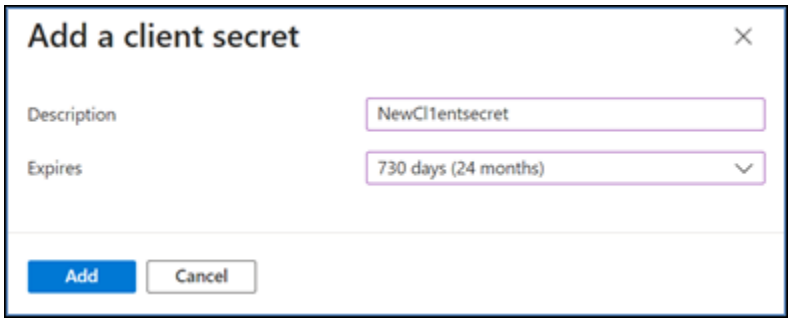
4. Choisissez Enregistrer.



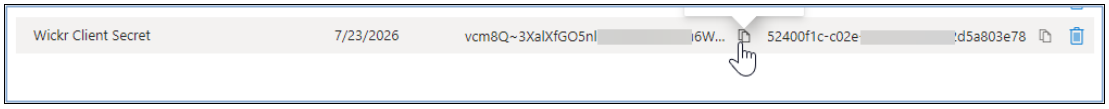
Étape 3 : Configuration des certificats et des secrets

Suivez la procédure suivante pour configurer les certificats et les secrets dans Microsoft Entra.

1. Dans le volet de navigation, sélectionnez Certificates & secrets.
2. Sur la page Certificats et secrets, sélectionnez l'onglet Secrets clients.
3. Dans l'onglet Secret client, sélectionnez Nouveau secret client.
4. Entrez une description et sélectionnez une période d'expiration pour le secret.
5. Choisissez Ajouter.



6. Une fois le certificat créé, copiez la valeur secrète du client.

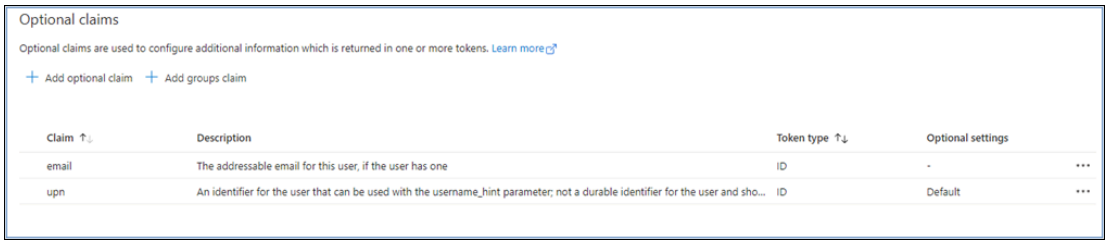


> **Note**
>
> La valeur secrète du client (et non l'ID secret) sera requise pour le code de votre application client. Il se peut que vous ne puissiez pas afficher ou copier la valeur secrète après avoir quitté cette page. Si vous ne le copiez pas maintenant, vous devrez y retourner pour créer un nouveau secret client.

Étape 4 : Configuration de la configuration du jeton

Suivez la procédure suivante pour configurer la configuration des jetons dans Microsoft Entra.

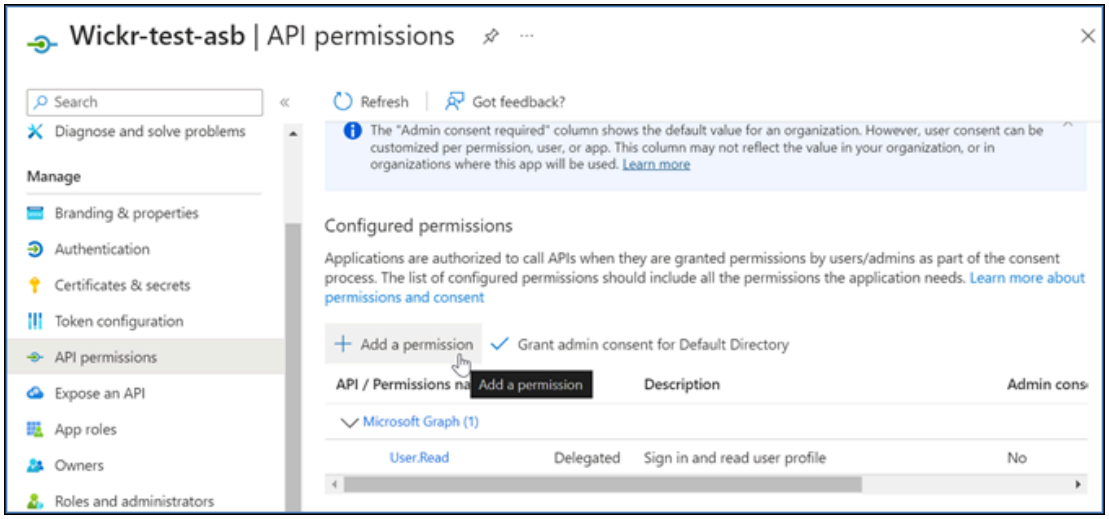
1. Dans le volet de navigation, choisissez Configuration du jeton.
2. Sur la page de configuration du jeton, choisissez Ajouter une réclamation facultative.
3. Sous Réclamations facultatives, sélectionnez le type de jeton comme identifiant.
4. Après avoir sélectionné l'identifiant, sous Réclamer, sélectionnez e-mail et UPN.
5. Choisissez Ajouter.



Étape 5 : Configuration des autorisations d'API

Suivez la procédure suivante pour configurer les autorisations d'API dans Microsoft Entra.

1. Dans le panneau de navigation, choisissez API permissions (Autorisations d'API).
2. Sur la page des autorisations de l'API, choisissez Ajouter une autorisation.

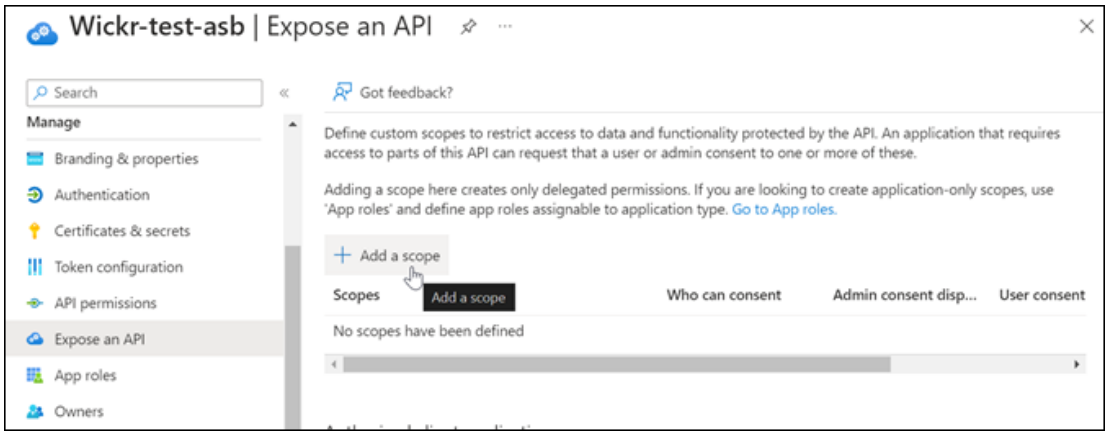


3. Sélectionnez Microsoft Graph, puis sélectionnez Autorisations déléguées.
4. Cochez la case pour e-mail, offline_access, openid, profile.
5. Choisissez Ajouter des autorisations.

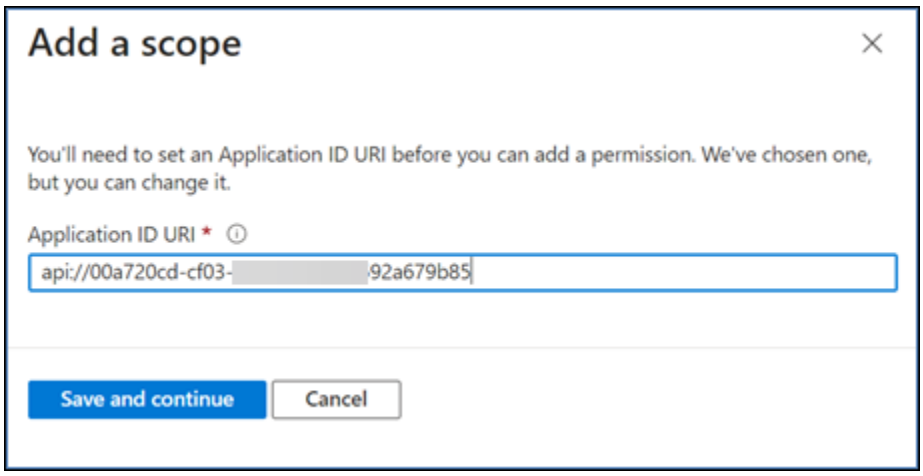
Étape 6 : exposer une API

Effectuez la procédure suivante pour exposer une API pour chacun des 4 champs d'application de Microsoft Entra.

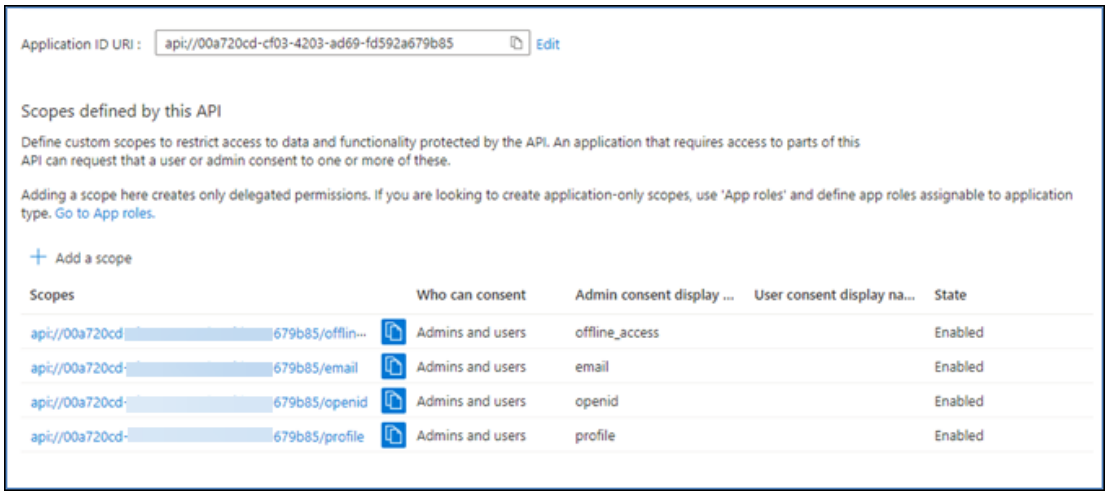
1. Dans le volet de navigation, choisissez Exposer une API.
2. Sur la page Exposer une API, choisissez Ajouter une portée.



L'URI de l'ID de l'application doit être renseignée automatiquement, et l'ID qui suit l'URI doit correspondre à l'ID de l'application (créé dans Register AWS Wickr en tant qu'application).



3. Choisissez Save and continue (Enregistrer et continuer).
4. Sélectionnez le tag Admins and users, puis entrez le nom de la portée sous la forme offline_access.
5. Sélectionnez État, puis sélectionnez Activer.
6. Choisissez Ajouter un champ d'application.
7. Répétez les étapes 1 à 6 de cette section pour ajouter les champs d'application suivants : e-mail, openid et profile.



8. Sous Applications clientes autorisées, sélectionnez Ajouter une application client.
9. Sélectionnez les quatre étendues créées à l'étape précédente.
10. Entrez ou vérifiez l'ID de l'application (client).
11. Choisissez Add application (Ajouter une application).

Étape 7 : configuration SSO d'AWS Wickr

Effectuez la procédure de configuration suivante dans la console AWS Wickr.

1. Ouvrez le AWS Management Console pour Wickr à l'adresse https://console.aws.amazon.com/wickr/.
2. Sur la page Réseaux, sélectionnez le nom du réseau pour accéder à ce réseau.
3. Dans le volet de navigation, choisissez Gestion des utilisateurs, puis sélectionnez Configurer l'authentification unique.
4. Entrez les détails suivants :

   - Émetteur — Il s'agit du point de terminaison qui a été modifié précédemment (par exemple`https://login.microsoftonline.com/1ce43025-e4b1-462d-a39f-337f20f1f4e1/v2.0/`).
   - ID client — Il s'agit de l'ID de l'application (client) indiqué dans le volet Vue d'ensemble.
   - Secret client (facultatif) — Il s'agit du secret client indiqué dans le volet Certificats et secrets.
   - Étendue : il s'agit des noms de portée exposés dans le volet Exposer une API. Entrez email, profile, offline_access et openid.
   - Étendue du nom d'utilisateur personnalisée (facultatif) — Entrez upn.
   - Numéro d'entreprise — Il peut s'agir d'une valeur de texte unique comprenant des caractères alphanumériques et des traits de soulignement. C'est cette phrase que vos utilisateurs saisiront lorsqu'ils s'enregistreront sur de nouveaux appareils.

   Les autres champs sont facultatifs.
5. Choisissez Suivant.
6. Vérifiez les informations dans la page Réviser et enregistrer, puis choisissez Enregistrer les modifications.

La configuration SSO est terminée. Pour vérifier, vous pouvez désormais ajouter un utilisateur à l'application dans Microsoft Entra et vous connecter avec cet utilisateur à l'aide de l'authentification unique et de l'identifiant d'entreprise.

Pour plus d'informations sur la façon d'inviter et d'intégrer des utilisateurs, voir Créer et inviter des utilisateurs.

Résolution des problèmes

Vous trouverez ci-dessous les problèmes courants que vous pourriez rencontrer et des suggestions pour les résoudre.

- Le test de connexion SSO échoue ou ne répond pas :
  - Assurez-vous que l'émetteur SSO est configuré comme prévu.
  - Assurez-vous que les champs obligatoires dans le SSO Configuré sont définis comme prévu.
- Le test de connexion est réussi, mais l'utilisateur ne parvient pas à se connecter :
  - Assurez-vous que l'utilisateur est ajouté à l'application Wickr que vous avez enregistrée dans Microsoft Entra.
  - Assurez-vous que l'utilisateur utilise le bon identifiant d'entreprise, y compris le préfixe. Par exemple, UE1 DemoNetwork W_drqtva.
  - Le secret du client n'est peut-être pas défini correctement dans la configuration SSO d'AWS Wickr. Réinitialisez-le en créant un autre secret client dans Microsoft Entra et définissez le nouveau secret client dans la configuration SSO de Wickr.

Période de grâce pour l'actualisation des jetons

Il peut arriver que les fournisseurs d'identité soient confrontés à des interruptions temporaires ou prolongées, ce qui peut entraîner la déconnexion inattendue de vos utilisateurs en raison de l'échec d'un jeton d'actualisation pour leur session client. Pour éviter ce problème, vous pouvez établir une période de grâce qui permet à vos utilisateurs de rester connectés même si leur jeton d'actualisation client échoue lors de telles pannes.

Voici les options disponibles pour la période de grâce :

- Aucune période de grâce (par défaut) : les utilisateurs seront déconnectés immédiatement après l'échec d'un jeton d'actualisation.
- Période de grâce de 30 minutes : les utilisateurs peuvent rester connectés jusqu'à 30 minutes après l'échec d'un jeton d'actualisation.
- Période de grâce de 60 minutes : les utilisateurs peuvent rester connectés pendant 60 minutes au maximum après l'échec d'un jeton d'actualisation.

Balises réseau pour AWS Wickr

Vous pouvez appliquer des tags aux réseaux Wickr. Vous pouvez ensuite utiliser ces balises pour rechercher et filtrer vos réseaux Wickr ou suivre vos AWS coûts. Vous pouvez configurer les balises réseau sur la page d'accueil du réseau AWS Management Console pour Wickr.

Une balise est une paire clé-valeur appliquée à une ressource pour contenir les métadonnées relatives à cette ressource. Chaque balise est une étiquette composée d'une clé et d'une valeur. Pour plus d'informations sur les balises, voir également Que sont les balises ? et les cas d'utilisation du balisage.

Rubriques

Gérer les balises réseau dans AWS Wickr

Vous pouvez gérer les balises réseau de votre réseau Wickr.

Suivez la procédure suivante pour gérer les balises réseau de votre réseau Wickr.

1. Ouvrez le AWS Management Console pour Wickr à l'adresse https://console.aws.amazon.com/wickr/.
2. Sur la page Réseaux, sélectionnez le nom du réseau pour accéder à ce réseau.
3. Sur la page d'accueil du réseau, dans la section Balises, choisissez Gérer les balises.
4. Sur la page Gérer les balises, vous pouvez effectuer l'une des options suivantes :

    - Ajouter de nouvelles balises — Entrez de nouvelles balises sous la forme d'une clé et d'une paire de valeurs. Choisissez Ajouter une nouvelle balise pour ajouter plusieurs paires clé-valeur. Les balises sont sensibles à la casse. Pour de plus amples informations, veuillez consulter Ajouter une balise réseau dans AWS Wickr.
    - Modifier les balises existantes : sélectionnez le texte de clé ou de valeur d'une balise existante, puis entrez la modification dans la zone de texte. Pour de plus amples informations, veuillez consulter Modifier une balise réseau dans AWS Wickr.

- Supprimer les balises existantes : cliquez sur le bouton Supprimer qui se trouve à côté de la balise que vous souhaitez supprimer. Pour de plus amples informations, veuillez consulter Supprimer une balise réseau dans AWS Wickr.

Ajouter une balise réseau dans AWS Wickr

Vous pouvez ajouter un tag réseau à votre réseau Wickr.

Suivez la procédure suivante pour ajouter un tag à votre réseau Wickr. Pour plus d'informations sur la gestion des balises, consultezGérer les balises réseau dans AWS Wickr.

1. Sur la page d'accueil du réseau, dans la section Balises, choisissez Ajouter une nouvelle balise.
2. Sur la page Gérer les balises, choisissez Ajouter une nouvelle balise.
3. Dans les champs vides de clé et de valeur qui apparaissent, entrez la nouvelle clé et la nouvelle valeur de balise.
4. Choisissez Enregistrer les modifications pour enregistrer les nouvelles balises.

Modifier une balise réseau dans AWS Wickr

Vous pouvez modifier un tag réseau sur votre réseau Wickr.

Suivez la procédure suivante pour modifier un tag associé à votre réseau Wickr. Pour plus d'informations sur la gestion des balises, consultezGérer les balises réseau dans AWS Wickr.

1. Sur la page Gérer les balises, modifiez la valeur d'une balise.

   > **Note**
   >
   > Vous ne pouvez pas modifier la clé d'un tag. Supprimez plutôt la paire clé/valeur et ajoutez une nouvelle balise à l'aide de la nouvelle clé.

2. Choisissez Enregistrer les modifications pour enregistrer vos modifications.

Supprimer une balise réseau dans AWS Wickr

Vous pouvez supprimer un tag réseau de votre réseau Wickr.

Effectuez la procédure suivante pour supprimer un tag de votre réseau Wickr. Pour plus d'informations sur la gestion des balises, consultezGérer les balises réseau dans AWS Wickr.

1. Sur la page Gérer les balises, choisissez Supprimer pour la balise que vous souhaitez supprimer.
2. Choisissez Enregistrer les modifications pour enregistrer vos modifications.

Lire les reçus pour AWS Wickr

Les accusés de lecture pour AWS Wickr sont des notifications envoyées à l'expéditeur pour indiquer quand son message a été lu. Ces reçus sont disponibles dans les one-on-one conversations. Une seule coche apparaît pour les messages envoyés, et un cercle plein avec une coche apparaît pour les messages lus. Pour voir les accusés de lecture sur les messages lors de conversations externes, les accusés de lecture doivent être activés sur les deux réseaux.

Les administrateurs peuvent activer ou désactiver les confirmations de lecture dans le panneau de configuration de l'administrateur. Ce paramètre sera appliqué à l'ensemble du réseau.

Procédez comme suit pour activer ou désactiver les confirmations de lecture.

1. Ouvrez le AWS Management Console pour Wickr à l'adresse https://console.aws.amazon.com/wickr/.
2. Sur la page Réseaux, sélectionnez le nom du réseau pour accéder à ce réseau.
3. Dans le volet de navigation, sélectionnez Network policies.
4. Sur la page Politiques réseau, dans la section Messagerie, choisissez Modifier.
5. Cochez la case pour activer ou désactiver les confirmations de lecture.
6. Sélectionnez Enregistrer les modifications.

Gérer le plan réseau pour AWS Wickr

Dans AWS Management Console for Wickr, vous pouvez gérer votre plan réseau en fonction des besoins de votre entreprise.

Pour gérer votre plan réseau, procédez comme suit.

1. Ouvrez le AWS Management Console pour Wickr à l'adresse https://console.aws.amazon.com/wickr/.

2. Sur la page Réseaux, sélectionnez le nom du réseau pour accéder à ce réseau.
3. Sur la page d'accueil du réseau, dans la section Détails du réseau, choisissez Modifier.
4. Sur la page Modifier les détails du réseau, choisissez le plan réseau de votre choix. Vous pouvez modifier votre plan réseau actuel en choisissant l'une des options suivantes :

   - Standard — Pour les équipes des petites et grandes entreprises qui ont besoin de contrôles administratifs et de flexibilité.
   - Essai gratuit Premium ou Premium : pour les entreprises qui ont besoin des limites de fonctionnalités les plus élevées, de contrôles administratifs précis et de la conservation des données.

     Les administrateurs ont la possibilité de sélectionner un essai gratuit premium, disponible pour un maximum de 30 utilisateurs et d'une durée de trois mois. En AWS WickrGov effet, l'option d'essai gratuit premium permet jusqu'à 50 utilisateurs et dure également trois mois. Cette offre est ouverte aux nouveaux forfaits et aux forfaits standard. Pendant la période d'essai gratuite Premium, les administrateurs peuvent passer à un forfait Premium ou Standard ou à un abonnement inférieur.

     > **Note**
     >
     > Pour arrêter l'utilisation et la facturation sur votre réseau, supprimez tous les utilisateurs, y compris les utilisateurs suspendus de votre réseau.

Limitations de l'essai gratuit Premium

Les restrictions suivantes s'appliquent à l'essai gratuit premium :

- Si un plan a déjà été inscrit à un essai gratuit premium auparavant, il ne sera pas éligible à un autre essai.
- Un seul réseau pour chaque AWS compte peut être inscrit à un essai gratuit premium.
- La fonctionnalité d'utilisateur invité n'est pas disponible pendant l'essai gratuit Premium.
- Si un réseau standard compte plus de 30 utilisateurs (plus de 50 utilisateurs pour AWS WickrGov), il ne sera pas possible de passer à un essai gratuit premium.

Conservation des données pour AWS Wickr

La conservation des données AWS Wickr permet de conserver toutes les conversations sur le réseau. Cela inclut les conversations par message direct et les conversations dans des groupes ou des salles entre les membres du réseau (internes) et ceux avec d'autres équipes (externes) avec lesquelles votre réseau est fédéré. La conservation des données n'est disponible que pour les utilisateurs du plan AWS Wickr Premium et les clients professionnels qui optent pour la conservation des données. Pour plus d'informations sur le plan Premium, consultez les tarifs de Wickr

Lorsqu'un administrateur réseau configure et active la conservation des données pour son réseau, tous les messages et fichiers partagés sur son réseau sont conservés conformément aux politiques de conformité de l'organisation. Ces sorties de fichiers .txt sont accessibles par l'administrateur réseau depuis un emplacement externe (par exemple : stockage local, compartiment Amazon S3 ou tout autre stockage selon le choix de l'utilisateur), d'où elles peuvent être analysées, effacées ou transférées.

> **Note**
>
> Wickr n'accède jamais à vos messages et à vos fichiers. Il est donc de votre responsabilité de configurer un système de conservation des données.

Rubriques

Afficher les détails relatifs à la conservation des données dans AWS Wickr

Suivez la procédure suivante pour consulter les détails de conservation des données pour votre réseau Wickr. Vous pouvez également activer ou désactiver la conservation des données pour votre réseau Wickr.

1. Ouvrez le AWS Management Console pour Wickr à l'adresse https://console.aws.amazon.com/wickr/.

2. Sur la page Réseaux, sélectionnez le nom du réseau pour accéder à ce réseau.
3. Dans le volet de navigation, sélectionnez Network policies.
4. La page des politiques réseau affiche les étapes de configuration de la conservation des données, ainsi que la possibilité d'activer ou de désactiver la fonctionnalité de conservation des données. Pour plus d'informations sur la configuration de la conservation des données, consultezConfiguration de la conservation des données pour AWS Wickr.

> **Note**
>
> Lorsque la conservation des données est activée, un message indiquant que la conservation des données est activée sera visible pour tous les utilisateurs de votre réseau pour les informer de l'existence du réseau activé.

Configuration de la conservation des données pour AWS Wickr

Pour configurer la conservation des données pour votre réseau AWS Wickr, vous devez déployer l'image Docker du bot de conservation des données dans un conteneur sur un hôte, tel qu'un ordinateur local ou une instance dans Amazon Elastic Compute Cloud (Amazon EC2). Une fois le bot déployé, vous pouvez le configurer pour stocker les données localement ou dans un bucket Amazon Simple Storage Service (Amazon S3). Vous pouvez également configurer le bot de conservation des données pour utiliser d'autres AWS services tels que AWS Secrets Manager (Secrets Manager), Amazon CloudWatch (CloudWatch), Amazon Simple Notification Service (Amazon SNS) et (). AWS Key Management Service AWS KMS Les rubriques suivantes décrivent comment configurer et exécuter le bot de conservation des données pour votre réseau Wickr.

Rubriques

Conditions préalables à la configuration de la conservation des données pour AWS Wickr

Avant de commencer, vous devez obtenir le nom du bot de conservation des données (étiqueté comme nom d'utilisateur) et le mot de passe initial auprès de AWS Management Console for Wickr. Vous devez spécifier ces deux valeurs la première fois que vous démarrez le bot de conservation des données. Vous devez également activer la conservation des données dans la console. Pour de plus amples informations, veuillez consulter Afficher les détails relatifs à la conservation des données dans AWS Wickr.

Mot de passe pour le bot de conservation des données dans AWS Wickr

La première fois que vous démarrez le bot de conservation des données, vous spécifiez le mot de passe initial à l'aide de l'une des options suivantes :

- Variable d'environnement `WICKRIO_BOT_PASSWORD`. Les variables d'environnement du bot de conservation des données sont décrites dans la Variables d'environnement pour configurer le bot de conservation des données dans AWS Wickr section suivante de ce guide.
- La valeur du mot de passe dans Secrets Manager identifiée par la variable d'`AWS_SECRET_NAME`environnement. Les valeurs de Secrets Manager pour le bot de conservation des données sont décrites dans la Les valeurs de Secrets Manager pour AWS Wickr section suivante de ce guide.
- Entrez le mot de passe lorsque le bot de conservation des données vous le demande. Vous devrez exécuter le bot de conservation des données avec un accès TTY interactif à l'aide de l'`-ti`option.

Un nouveau mot de passe sera généré lorsque vous configurerez le bot de conservation des données pour la première fois. Si vous devez réinstaller le bot de conservation des données, vous devez utiliser le mot de passe généré. Le mot de passe initial n'est pas valide après l'installation initiale du bot de conservation des données.

Le nouveau mot de passe généré sera affiché comme indiqué dans l'exemple suivant.

> **Important**
>
> Conservez le mot de passe en lieu sûr. Si vous perdez le mot de passe, vous ne pourrez pas réinstaller le bot de conservation des données. Ne partagez pas ce mot de passe. Il permet de démarrer la conservation des données pour votre réseau Wickr.

```
*****************************************************************
**** GENERATED PASSWORD
**** DO NOT LOSE THIS PASSWORD, YOU WILL NEED TO ENTER IT EVERY TIME
**** TO START THE BOT
 "HuEXAMPLERAW4lGgEXAMPLEn"
 *****************************************************************
```

Options de stockage pour le réseau AWS Wickr

Une fois la conservation des données activée et le bot de conservation des données configuré pour votre réseau Wickr, il capturera tous les messages et fichiers envoyés sur votre réseau. Les messages sont enregistrés dans des fichiers limités à une taille ou à une durée spécifiques qui peuvent être configurées à l'aide d'une variable d'environnement. Pour de plus amples informations, veuillez consulter Variables d'environnement pour configurer le bot de conservation des données dans AWS Wickr.

Vous pouvez configurer l'une des options suivantes pour stocker ces données :

- Stockez tous les messages et fichiers capturés localement. Il s'agit de l'option par défaut. Il est de votre responsabilité de déplacer les fichiers locaux vers un autre système pour un stockage à long terme et de vous assurer que le disque hôte ne manque pas de mémoire ou d'espace.
- Stockez tous les messages et fichiers capturés dans un compartiment Amazon S3. Le bot de conservation des données enregistre tous les messages et fichiers déchiffrés dans le compartiment Amazon S3 que vous spécifiez. Les messages et fichiers capturés sont supprimés de la machine hôte une fois qu'ils ont été correctement enregistrés dans le compartiment.
- Stockez tous les messages et fichiers capturés chiffrés dans un compartiment Amazon S3. Le bot de conservation des données chiffre à nouveau tous les messages et fichiers capturés à l'aide d'une clé que vous fournissez et les enregistre dans le compartiment Amazon S3 que vous spécifiez. Les messages et fichiers capturés sont supprimés de la machine hôte une fois qu'ils ont été correctement rechiffrés et enregistrés dans le compartiment. Vous aurez besoin d'un logiciel pour déchiffrer les messages et les fichiers.

  Pour plus d'informations sur la création d'un compartiment Amazon S3 à utiliser avec votre bot de conservation des données, consultez la section Création d'un compartiment dans le guide de l'utilisateur Amazon S3

Variables d'environnement pour configurer le bot de conservation des données dans AWS Wickr

Vous pouvez utiliser les variables d'environnement suivantes pour configurer le bot de conservation des données. Vous définissez ces variables d'environnement à l'aide de l'`-e`option lorsque vous exécutez l'image Docker du bot de conservation des données. Pour de plus amples informations, veuillez consulter Démarrez le bot de conservation des données pour votre réseau Wickr.

> **Note**
>
> Ces variables d'environnement sont facultatives, sauf indication contraire.

Utilisez les variables d'environnement suivantes pour spécifier les informations d'identification du bot de conservation des données :

- `WICKRIO_BOT_NAME`— Le nom du bot de conservation des données. Cette variable est obligatoire lorsque vous exécutez l'image Docker du bot de conservation des données.
- `WICKRIO_BOT_PASSWORD`— Le mot de passe initial du bot de conservation des données. Pour de plus amples informations, veuillez consulter Conditions préalables à la configuration de la conservation des données pour AWS Wickr. Cette variable est obligatoire si vous ne prévoyez pas de démarrer le bot de conservation des données en demandant un mot de passe ou si vous ne prévoyez pas d'utiliser Secrets Manager pour stocker les informations d'identification du bot de conservation des données.

Utilisez les variables d'environnement suivantes pour configurer les fonctionnalités de streaming de conservation des données par défaut :

- `WICKRIO_COMP_MESGDEST`— Le nom du chemin d'accès au répertoire dans lequel les messages seront diffusés. La valeur par défaut est `/tmp/<botname>/compliance/messages`.
- `WICKRIO_COMP_FILEDEST`— Le nom du chemin d'accès au répertoire dans lequel les fichiers seront diffusés. La valeur par défaut est `/tmp/<botname>/compliance/attachments`.
- `WICKRIO_COMP_BASENAME`— Le nom de base des fichiers de messages reçus. La valeur par défaut est `receivedMessages`.
- `WICKRIO_COMP_FILESIZE`— La taille maximale d'un fichier de messages reçus en kibioctet (KiB). Un nouveau fichier est lancé lorsque la taille maximale est atteinte. La valeur par défaut est`1000000000`, comme dans 1024 GiB.

- `WICKRIO_COMP_TIMEROTATE`— Durée, en minutes, pendant laquelle le bot de conservation des données insère les messages reçus dans un fichier de messages reçus. Un nouveau fichier est lancé lorsque le délai est atteint. Vous ne pouvez utiliser la taille ou la durée du fichier que pour limiter la taille du fichier des messages reçus. La valeur par défaut est`0`, comme dans aucune limite.

Utilisez la variable d'environnement suivante pour définir la valeur par défaut Région AWS à utiliser.

- `AWS_DEFAULT_REGION`— La valeur par défaut Région AWS à utiliser pour AWS des services tels que Secrets Manager (non utilisée pour Amazon S3 ou AWS KMS). La `us-east-1` région est utilisée par défaut si cette variable d'environnement n'est pas définie.

Utilisez les variables d'environnement suivantes pour spécifier le secret Secrets Manager à utiliser lorsque vous choisissez d'utiliser Secrets Manager pour stocker les informations d'identification et les informations de AWS service du bot de conservation des données. Pour plus d'informations sur les valeurs que vous pouvez stocker dans Secrets Manager, consultezLes valeurs de Secrets Manager pour AWS Wickr.

- `AWS_SECRET_NAME`— Le nom du secret Secrets Manager qui contient les informations d'identification et AWS de service nécessaires au bot de conservation des données.
- `AWS_SECRET_REGION`— L' Région AWS endroit où se trouve le AWS secret. Si vous utilisez des AWS secrets et que cette valeur n'est pas définie, la `AWS_DEFAULT_REGION` valeur sera utilisée.

> **Note**
>
> Vous pouvez stocker toutes les variables d'environnement suivantes sous forme de valeurs dans Secrets Manager. Si vous choisissez d'utiliser Secrets Manager et que vous y stockez ces valeurs, vous n'avez pas besoin de les spécifier en tant que variables d'environnement lorsque vous exécutez l'image Docker du bot de conservation des données. Il vous suffit de spécifier la variable d'`AWS_SECRET_NAME`environnement décrite plus haut dans ce guide. Pour de plus amples informations, veuillez consulter Les valeurs de Secrets Manager pour AWS Wickr.

Utilisez les variables d'environnement suivantes pour spécifier le compartiment Amazon S3 lorsque vous choisissez de stocker des messages et des fichiers dans un compartiment.

- `WICKRIO_S3_BUCKET_NAME`— Le nom du compartiment Amazon S3 dans lequel les messages et les fichiers seront stockés.
- `WICKRIO_S3_REGION`— La AWS région du compartiment Amazon S3 dans laquelle les messages et les fichiers seront stockés.
- `WICKRIO_S3_FOLDER_NAME`— Le nom du dossier facultatif dans le compartiment Amazon S3 où les messages et les fichiers seront stockés. Ce nom de dossier sera précédé de la clé pour les messages et les fichiers enregistrés dans le compartiment Amazon S3.

Utilisez les variables d'environnement suivantes pour spécifier les AWS KMS détails lorsque vous choisissez d'utiliser le chiffrement côté client pour rechiffrer les fichiers lorsque vous les enregistrez dans un compartiment Amazon S3.

- `WICKRIO_KMS_MSTRKEY_ARN`— Le nom de ressource Amazon (ARN) de la clé AWS KMS principale utilisée pour rechiffrer les fichiers de messages et les fichiers sur le bot de conservation des données avant qu'ils ne soient enregistrés dans le compartiment Amazon S3.
- `WICKRIO_KMS_REGION`— La AWS région où se trouve la clé AWS KMS principale.

Utilisez la variable d'environnement suivante pour spécifier les détails d'Amazon SNS lorsque vous choisissez d'envoyer des événements de rétention de données à une rubrique Amazon SNS. Les événements envoyés incluent le démarrage, l'arrêt, ainsi que les conditions d'erreur.

- `WICKRIO_SNS_TOPIC_ARN`— L'ARN de la rubrique Amazon SNS à laquelle vous souhaitez que les événements de conservation des données soient envoyés.

Utilisez la variable d'environnement suivante pour envoyer les métriques de conservation des données à CloudWatch. Si cela est spécifié, les métriques seront générées toutes les 60 secondes.

- `WICKRIO_METRICS_TYPE`— Définissez la valeur de cette variable d'environnement `cloudwatch` à laquelle envoyer les métriques CloudWatch.

Les valeurs de Secrets Manager pour AWS Wickr

Vous pouvez utiliser Secrets Manager pour stocker les informations d'identification du bot de conservation des données et les informations AWS de service. Pour plus d'informations sur la création d'un secret Secrets Manager, voir Création d'un AWS Secrets Manager secret dans le Guide de l'utilisateur de Secrets Manager.

Le secret Secrets Manager peut avoir les valeurs suivantes :

- `password`— Le mot de passe du bot de conservation des données.
- `s3_bucket_name`— Le nom du compartiment Amazon S3 dans lequel les messages et les fichiers seront stockés. Si ce n'est pas le cas, le streaming de fichiers par défaut sera utilisé.
- `s3_region`— La AWS région du compartiment Amazon S3 dans laquelle les messages et les fichiers seront stockés.
- `s3_folder_name`— Le nom du dossier facultatif dans le compartiment Amazon S3 où les messages et les fichiers seront stockés. Ce nom de dossier sera précédé de la clé pour les messages et les fichiers enregistrés dans le compartiment Amazon S3.
- `kms_master_key_arn`— L'ARN de la clé AWS KMS principale utilisée pour rechiffrer les fichiers de messages et les fichiers sur le bot de conservation des données avant leur enregistrement dans le compartiment Amazon S3.
- `kms_region`— La AWS région où se trouve la clé AWS KMS principale.
- `sns_topic_arn`— L'ARN de la rubrique Amazon SNS à laquelle vous souhaitez que les événements de conservation des données soient envoyés.

Politique IAM pour utiliser la conservation des données avec les services AWS

Si vous envisagez d'utiliser d'autres AWS services avec le bot de conservation des données Wickr, vous devez vous assurer que l'hôte dispose du rôle et de la politique Gestion des identités et des accès AWS (IAM) appropriés pour y accéder. Vous pouvez configurer le bot de conservation des données pour utiliser Secrets Manager, Amazon S3 CloudWatch, Amazon SNS et. AWS KMS La politique IAM suivante permet d'accéder à des actions spécifiques pour ces services.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "s3:PutObject",
                "secretsmanager:GetSecretValue",
                "sns:Publish",
```

```
                "cloudwatch:PutMetricData",
                "kms:GenerateDataKey"
            ],
            "Resource": "*"
        }
    ]
}
```

Vous pouvez créer une politique IAM plus stricte en identifiant les objets spécifiques pour chaque service auxquels vous souhaitez autoriser les conteneurs de votre hôte à accéder. Supprimez les actions relatives aux AWS services que vous n'avez pas l'intention d'utiliser. Par exemple, si vous avez l'intention de n'utiliser qu'un compartiment Amazon S3, appliquez la politique suivante, qui supprime les `cloudwatch:PutMetricData` actions `secretsmanager:GetSecretValue` `sns:Publishkms:GenerateDataKey`,, et.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": "s3:PutObject",
            "Resource": "*"
        }
    ]
}
```

Si vous utilisez une instance Amazon Elastic Compute Cloud (Amazon EC2) pour héberger votre bot de conservation des données, créez un rôle IAM en utilisant le cas courant Amazon EC2 et attribuez une politique en utilisant la définition de politique ci-dessus.

Démarrez le bot de conservation des données pour votre réseau Wickr

Avant d'exécuter le bot de conservation des données, vous devez déterminer comment vous souhaitez le configurer. Si vous envisagez d'exécuter le bot sur un hôte qui :

- Vous n'aurez pas accès aux AWS services, vos options sont alors limitées. Dans ce cas, vous utiliserez les options de diffusion de messages par défaut. Vous devez décider si vous souhaitez limiter la taille des fichiers de messages capturés à une taille ou à un intervalle de temps spécifiques. Pour de plus amples informations, veuillez consulter Variables d'environnement pour configurer le bot de conservation des données dans AWS Wickr.
- Si vous aurez accès aux AWS services, vous devez créer un secret Secrets Manager pour stocker les informations d'identification du bot et les détails de configuration des AWS services. Une fois les AWS services configurés, vous pouvez démarrer l'image Docker du bot de conservation des données. Pour plus d'informations sur les informations que vous pouvez stocker dans un secret de Secrets Manager, voir Les valeurs de Secrets Manager pour AWS Wickr

Les sections suivantes présentent des exemples de commandes permettant d'exécuter l'image Docker du bot de conservation des données. Dans chacun des exemples de commandes, remplacez les valeurs d'exemple suivantes par les vôtres :

- *compliance_1234567890_bot*avec le nom de votre robot de conservation des données.
- *password*avec le mot de passe de votre robot de conservation des données.
- *wickr/data/retention/bot*avec le nom de votre secret Secrets Manager à utiliser avec votre bot de conservation des données.
- *bucket-name*avec le nom du compartiment Amazon S3 dans lequel les messages et les fichiers seront stockés.
- *folder-name*avec le nom du dossier dans le compartiment Amazon S3 dans lequel les messages et les fichiers seront stockés.
- *us-east-1*avec la AWS région de la ressource que vous spécifiez. Par exemple, la région de la clé AWS KMS principale ou la région du compartiment Amazon S3.
- *arn:aws:kms:us-east-1:111122223333:key/12345678-1234-abcde-a617-abababababab*avec l'Amazon Resource Name (ARN) de votre clé AWS KMS principale à utiliser pour rechiffrer les fichiers de messages et les fichiers.

Démarrez le bot avec une variable d'environnement de mot de passe (aucun AWS service)

La commande Docker suivante démarre le bot de conservation des données. Le mot de passe est spécifié à l'aide de la variable d'`WICKRIO_BOT_PASSWORD`environnement. Le bot commence à utiliser le streaming de fichiers par défaut et les valeurs par défaut définies dans la Variables

d'environnement pour configurer le bot de conservation des données dans AWS Wickr section de ce guide.

```
docker run -v /opt/compliance_1234567890_bot:/tmp/compliance_1234567890_bot \
-d --restart on-failure:5 --name="compliance_1234567890_bot" -ti \
-e WICKRIO_BOT_NAME='compliance_1234567890_bot' \
-e WICKRIO_BOT_PASSWORD='password' \
wickr/bot-compliance-cloud:latest
```

Démarrez le bot avec une demande de mot de passe (aucun AWS service)

La commande Docker suivante démarre le bot de conservation des données. Le mot de passe est saisi lorsque le bot de conservation des données vous le demande. Il commencera à utiliser le streaming de fichiers par défaut en utilisant les valeurs par défaut définies dans la Variables d'environnement pour configurer le bot de conservation des données dans AWS Wickr section de ce guide.

```
docker run -v /opt/compliance_1234567890_bot:/tmp/compliance_1234567890_bot \
-d --restart on-failure:5 --name="compliance_1234567890_bot" -ti \
-e WICKRIO_BOT_NAME='compliance_1234567890_bot' \
wickr/bot-compliance-cloud:latest

docker attach compliance_1234567890_bot
.
.
.
Enter the password:************
Re-enter the password:************
```

Exécutez le bot à l'aide de l'`-ti`option permettant de recevoir l'invite de mot de passe. Vous devez également exécuter la `docker attach` *`<container ID or container name>`* commande immédiatement après le démarrage de l'image docker afin de recevoir l'invite de mot de passe. Vous devez exécuter ces deux commandes dans un script. Si vous joignez l'image du docker et que vous ne voyez pas l'invite, appuyez sur Entrée pour afficher l'invite.

Démarrez le bot avec une rotation des fichiers de messages de 15 minutes (aucun AWS service)

La commande Docker suivante démarre le bot de conservation des données à l'aide de variables d'environnement. Il le configure également pour faire pivoter les fichiers de messages reçus à 15 minutes.

```
docker run -v /opt/compliance_1234567890_bot:/tmp/compliance_1234567890_bot --
network=host \
-d --restart on-failure:5 --name="compliance_1234567890_bot" -ti \
-e WICKRIO_BOT_NAME='compliance_1234567890_bot' \
-e WICKRIO_BOT_PASSWORD='password' \
-e WICKRIO_COMP_TIMEROTATE=15 \
wickr/bot-compliance-cloud:latest
```

Démarrez le bot et spécifiez le mot de passe initial avec Secrets Manager

Vous pouvez utiliser le Secrets Manager pour identifier le mot de passe du bot de conservation des données. Lorsque vous démarrez le bot de conservation des données, vous devez définir une variable d'environnement qui indique le Secrets Manager dans lequel ces informations sont stockées.

```
docker run -v /opt/compliance_1234567890_bot:/tmp/compliance_1234567890_bot --
network=host \
-d --restart on-failure:5 --name="compliance_1234567890_bot" -ti \
-e WICKRIO_BOT_NAME='compliance_1234567890_bot' \
-e AWS_SECRET_NAME='wickrpro/alpha/new-3-bot' \
wickr/bot-compliance-cloud:latest
```

Le `wickrpro/compliance/compliance_1234567890_bot` secret contient la valeur secrète suivante, affichée sous forme de texte brut.

```
{
    "password":"password"
}
```

Démarrez le bot et configurez Amazon S3 avec Secrets Manager

Vous pouvez utiliser le Secrets Manager pour héberger les informations d'identification et les informations du compartiment Amazon S3. Lorsque vous démarrez le bot de conservation des données, vous devez définir une variable d'environnement qui indique le Secrets Manager dans lequel ces informations sont stockées.

```
docker run -v /opt/compliance_1234567890_bot:/tmp/compliance_1234567890_bot --
network=host \
-d --restart on-failure:5 --name="compliance_1234567890_bot" -ti \
 -e WICKRIO_BOT_NAME='compliance_1234567890_bot' \
 -e AWS_SECRET_NAME='wickrpro/alpha/compliance_1234567890_bot' \
```

```
wickr/bot-compliance-cloud:latest
```

Le `wickrpro/compliance/compliance_1234567890_bot` secret contient la valeur secrète suivante, affichée sous forme de texte brut.

```
{
    "password":"password",
    "s3_bucket_name":"bucket-name",
    "s3_region":"us-east-1",
    "s3_folder_name":"folder-name"
}
```

Les messages et les fichiers reçus par le bot seront placés dans le `bot-compliance` compartiment du dossier nomméne`twork1234567890`.

Démarrez le bot et configurez Amazon S3 et AWS KMS avec Secrets Manager

Vous pouvez utiliser le Secrets Manager pour héberger les informations d'identification, le compartiment Amazon S3 et les informations relatives à la clé AWS KMS principale. Lorsque vous démarrez le bot de conservation des données, vous devez définir une variable d'environnement qui indique le Secrets Manager dans lequel ces informations sont stockées.

```
docker run -v /opt/compliance_1234567890_bot:/tmp/compliance_1234567890_bot --
network=host \
-d --restart on-failure:5 --name="compliance_1234567890_bot" -ti \
 -e WICKRIO_BOT_NAME='compliance_1234567890_bot' \
 -e AWS_SECRET_NAME='wickrpro/alpha/compliance_1234567890_bot' \
wickr/bot-compliance-cloud:latest
```

Le `wickrpro/compliance/compliance_1234567890_bot` secret contient la valeur secrète suivante, affichée sous forme de texte brut.

```
{
    "password":"password",
    "s3_bucket_name":"bucket-name",
    "s3_region":"us-east-1",
    "s3_folder_name":"folder-name",
    "kms_master_key_arn":"arn:aws:kms:us-east-1:111122223333:key/12345678-1234-abcde-
a617-abababababab",
    "kms_region":"us-east-1"
}
```

Les messages et les fichiers reçus par le bot seront chiffrés à l'aide de la clé KMS identifiée par la valeur ARN, puis placés dans le compartiment « bot-compliance » dans le dossier nommé « network1234567890 ». Assurez-vous de disposer de la configuration de politique IAM appropriée.

Démarrez le bot et configurez Amazon S3 à l'aide de variables d'environnement

Si vous ne souhaitez pas utiliser Secrets Manager pour héberger les informations d'identification du bot de conservation des données, vous pouvez démarrer l'image Docker du bot de conservation des données avec les variables d'environnement suivantes. Vous devez identifier le nom du bot de conservation des données à l'aide de la variable d'`WICKRIO_BOT_NAME`environnement.

```
docker run -v /opt/compliance_1234567890_bot:/tmp/compliance_1234567890_bot --
network=host \
-d --restart on-failure:5 --name="compliance_1234567890_bot" -ti \
-e WICKRIO_BOT_NAME='compliance_1234567890_bot' \
-e WICKRIO_BOT_PASSWORD='password' \
-e WICKRIO_S3_BUCKET_NAME='bot-compliance' \
-e WICKRIO_S3_FOLDER_NAME='network1234567890' \
-e WICKRIO_S3_REGION='us-east-1' \
wickr/bot-compliance-cloud:latest
```

Vous pouvez utiliser les valeurs d'environnement pour identifier les informations d'identification du bot de conservation des données, les informations sur les compartiments Amazon S3 et les informations de configuration pour le streaming de fichiers par défaut.

Arrêtez le bot de conservation des données pour votre réseau Wickr

Le logiciel exécuté sur le bot de conservation des données capturera les `SIGTERM` signaux et s'arrêtera harmonieusement. Utilisez la `docker stop` *`<container ID or container name>`* commande, comme indiqué dans l'exemple suivant, pour envoyer la `SIGTERM` commande à l'image Docker du bot de conservation des données.

```
docker stop compliance_1234567890_bot
```

Obtenez les journaux de conservation des données pour votre réseau Wickr

Le logiciel exécuté sur l'image Docker du bot de conservation des données sera affiché dans les fichiers journaux du `/tmp/`*`<botname>`*`/logs` répertoire. Ils tourneront jusqu'à un maximum de 5 fichiers. Vous pouvez obtenir les journaux en exécutant la commande suivante.

```
docker logs <botname>
```

Exemple :

```
docker logs compliance_1234567890_bot
```

Mesures et événements de conservation des données pour votre réseau Wickr

Vous trouverez ci-dessous les métriques Amazon CloudWatch (CloudWatch) et les événements Amazon Simple Notification Service (Amazon SNS) actuellement pris en charge par la version 5.116 du bot de conservation des données AWS Wickr.

Rubriques

CloudWatch métriques pour votre réseau Wickr

Les métriques sont générées par le bot à intervalles d'une minute et transmises au CloudWatch service associé au compte sur lequel l'image Docker du bot de conservation des données est exécutée.

Vous trouverez ci-dessous les mesures existantes prises en charge par le bot de conservation des données.

Métrique	Description
Messages_Rx	Messages reçus.
Messages_Rx_Failed	Échec du traitement des messages reçus.
Messages enregistrés	Messages enregistrés dans le fichier des messages reçus.
Messages_enregistrés_échoués	Impossible d'enregistrer les messages dans le fichier des messages reçus.

Métrique	Description
Fichiers_enregistrés	Fichiers reçus.
Fichiers_enregistrés_octets	Nombre d'octets pour les fichiers reçus.
Les fichiers enregistrés ont échoué	Échec de l'enregistrement des fichiers.
Connexions	Connexions (normalement, ce sera 1 pour chaque intervalle).
Échecs de connexion	Échec de connexion (normalement, ce sera 1 pour chaque intervalle).
S3_Post_Errors	Erreurs lors de la publication de fichiers de messages et de fichiers dans le compartiment Amazon S3.
Watchdog_Failures	Défaillances de Watchdog.
Watchdog_Warnings	Avertissements de Watchdog.

Les métriques sont générées pour être consommées par CloudWatch. L'espace de noms utilisé pour les robots est`WickrIO`. Chaque métrique possède un ensemble de dimensions. Vous trouverez ci-dessous la liste des dimensions publiées avec les statistiques ci-dessus.

Dimension	Value
Id	Le nom d'utilisateur du bot.
Appareil	Description d'un appareil ou d'une instance de bot spécifique. Utile si vous utilisez plusieurs appareils ou instances de bot.
Produit (langue française non garantie)	Le produit pour le bot. Peut être `WickrPro_` ou `WickrEnterprise_` avec `AlphaBeta`, ou `Production` ajouté.

Dimension	Value
BotType	Le type de bot. Labellisé Conformité pour les robots de conformité.
Réseau	L'ID du réseau associé.

Événements Amazon SNS pour votre réseau Wickr

Les événements suivants sont publiés dans la rubrique Amazon SNS définie par la valeur Amazon Resource Name (ARN) identifiée à l'aide de la variable d'`WICKRIO_SNS_TOPIC_ARN`environnement ou de la valeur secrète de `sns_topic_arn` Secrets Manager. Pour plus d'informations, consultez Variables d'environnement pour configurer le bot de conservation des données dans AWS Wickr et Les valeurs de Secrets Manager pour AWS Wickr.

Les événements générés par le bot de conservation des données sont envoyés sous forme de chaînes JSON. Les valeurs suivantes sont incluses dans les événements à partir de la version 5.116 du bot de conservation des données.

Nom	Value
Bot de conformité	Le nom d'utilisateur du bot de conservation des données.
Heure des données	Date et heure auxquelles l'événement s'est produit.
device	Description de l'appareil ou de l'instance de bot spécifique. Utile si vous exécutez plusieurs instances de bot.
Image Docker	L'image Docker associée au bot.
Tag Docker	Le tag ou la version de l'image Docker.
message	Le message de l'événement. Pour plus d'informations, consultez Evénements critiques et Événements normaux.

Nom	Value
notificationType	Cette valeur sera`Bot Event`.
severity	La gravité de l'événement. Peut être `normal` ou `critical`.

Vous devez vous abonner à la rubrique Amazon SNS pour pouvoir recevoir les événements. Si vous vous abonnez à l'aide d'une adresse e-mail, un e-mail contenant des informations similaires à celles de l'exemple suivant vous sera envoyé.

```
{
"complianceBot": "compliance_1234567890_bot",
 "dateTime": "2022-10-12T13:05:39",
 "device": "Desktop 1234567890ab",
 "dockerImage": "wickr/bot-compliance-cloud",
 "dockerTag": "5.116.13.01",
 "message": "Logged in",
 "notificationType": "Bot Event",
 "severity": "normal"
}
```

Evénements critiques

Ces événements provoqueront l'arrêt ou le redémarrage du bot. Le nombre de redémarrages est limité afin d'éviter de provoquer d'autres problèmes.

Échecs de connexion

Voici les événements possibles qui peuvent être générés lorsque le bot ne parvient pas à se connecter. Chaque message indiquera la raison de l'échec de connexion.

Type d'événement	Message d'événement
échec de connexion	Mauvaises informations d'identification. Vérifiez le mot de passe.
échec de connexion	L'utilisateur n'a pas été trouvé.
échec de connexion	Le compte ou l'appareil est suspendu.

Type d'événement	Message d'événement
allocation	L'utilisateur a quitté la commande.
allocation	Mauvais mot de passe pour le `config.wickr` fichier.
allocation	Impossible de lire le `config.wickr` fichier.
échec de connexion	Toutes les connexions ont échoué.
échec de connexion	Nouvel utilisateur mais la base de données existe déjà.

Plus d'événements critiques

Type d'événement	Messages d'événements
Compte suspendu	Wickr IOClient Main : slotAdminUser Suspend : code (%1) : raison : %2 »
BotDevice Suspendu	L'appareil est suspendu !
WatchDog	Le SwitchBoard système est en panne pendant plus de < *N* > minutes
Défaillances S3	Impossible de placer le fichier < *file-name* ≫ dans le compartiment S3. Erreur : < *AWS-error* >
Clé de secours	CLÉ DE SECOURS SOUMISE PAR LE SERVEUR : Il ne s'agit pas d'une clé de secours active reconnue par le client. Veuillez envoyer les journaux à l'ingénierie de bureau.

Événements normaux

Vous trouverez ci-dessous les événements qui vous avertissent des événements de fonctionnement normaux. Un trop grand nombre d'événements de ce type au cours d'une période donnée peut être source de préoccupation.

Appareil ajouté au compte

Cet événement est généré lorsqu'un nouvel appareil est ajouté au compte du bot de conservation des données. Dans certaines circonstances, cela peut être une indication importante que quelqu'un a créé une instance du bot de conservation des données. Voici le message de cet événement.

```
A device has been added to this account!
```

Bot connecté

Cet événement est généré lorsque le bot s'est connecté avec succès. Voici le message de cet événement.

```
Logged in
```

Arrêt

Cet événement est généré lorsque le bot s'arrête. Si l'utilisateur ne l'a pas explicitement initié, cela peut être le signe d'un problème. Voici le message de cet événement.

```
Shutting down
```

Mises à jour disponibles

Cet événement est généré lorsque le bot de conservation des données est démarré et il indique qu'une version plus récente de l'image Docker associée est disponible. Cet événement est généré au démarrage du bot, et sur une base quotidienne. Cet événement inclut le champ du `versions` tableau qui identifie les nouvelles versions disponibles. Voici un exemple de ce à quoi ressemble cet événement.

```
{
  "complianceBot": "compliance_1234567890_bot",
  "dateTime": "2022-10-12T13:05:55",
  "device": "Desktop 1234567890ab",
```

```
  "dockerImage": "wickr/bot-compliance-cloud",
  "dockerTag": "5.116.13.01",
  "message": "There are updates available",
  "notificationType": "Bot Event",
  "severity": "normal",
  "versions": [
    "5.116.10.01"
  ]
}
```

Qu'est-ce qu'ATAK ?

L'Android Team Awareness Kit (ATAK), ou Android Tactical Assault Kit (également ATAK) à usage militaire, est une infrastructure géospatiale pour téléphones intelligents et une application de connaissance de la situation qui permettent une collaboration sécurisée sur tout le territoire. Bien qu'il ait été initialement conçu pour être utilisé dans les zones de combat, l'ATAK a été adapté aux missions des agences locales, étatiques et fédérales.

Rubriques

Activez ATAK dans le tableau de bord du réseau Wickr

AWS Wickr prend en charge de nombreuses agences qui utilisent Android Tactical Assault Kit (ATAK). Cependant, jusqu'à présent, les opérateurs ATAK qui utilisent Wickr devaient quitter l'application pour le faire. Pour aider à réduire les perturbations et les risques opérationnels, Wickr a développé un plugin qui améliore ATAK avec des fonctionnalités de communication sécurisées. Avec le plugin Wickr pour ATAK, les utilisateurs peuvent envoyer des messages, collaborer et transférer

des fichiers sur Wickr au sein de l'application ATAK. Cela élimine les interruptions et la complexité de la configuration grâce aux fonctionnalités de chat d'ATAK.

Activez ATAK dans le tableau de bord du réseau Wickr

Suivez la procédure suivante pour activer ATAK dans le tableau de bord du réseau Wickr.

1. Ouvrez le AWS Management Console pour Wickr à l'adresse https://console.aws.amazon.com/wickr/.
2. Sur la page Réseaux, sélectionnez le nom du réseau pour accéder à ce réseau.
3. Dans le panneau de navigation, choisissez Groupes de sécurité.
4. Sur la page Groupes de sécurité, sélectionnez le groupe de sécurité pour lequel vous souhaitez activer ATAK.
5. Dans l'onglet Intégration, dans la section du plugin ATAK, choisissez Modifier.
6. Sur la page Modifier le plugin ATAK, cochez la case Activer le plugin ATAK.
7. Choisissez Ajouter un nouveau package
8. Entrez le nom du package dans la zone de texte Packages. Vous pouvez entrer l'une des valeurs suivantes en fonction de la version de l'ATAK que vos utilisateurs vont installer et utiliser :

   - `com.atakmap.app.civ`— Entrez cette valeur dans la zone de texte Packages si vos utilisateurs finaux de Wickr veulent installer et utiliser la version civile de l'application ATAK sur leurs appareils Android.
   - `com.atakmap.app.mil`— Entrez cette valeur dans la zone de texte Packages si vos utilisateurs finaux de Wickr veulent installer et utiliser la version militaire de l'application ATAK sur leurs appareils Android.
9. Choisissez Enregistrer.

   ATAK est désormais activé pour le réseau Wickr sélectionné et le groupe de sécurité sélectionné. Vous devez demander aux utilisateurs Android du groupe de sécurité pour lequel vous avez activé la fonctionnalité ATAK d'installer le plugin Wickr pour ATAK. Pour plus d'informations, consultez Installer et associer le plugin Wickr ATAK.

Informations supplémentaires sur ATAK

Pour plus d'informations sur le plugin Wickr pour ATAK, consultez ce qui suit :

- Présentation du plugin Wickr ATAK

- Informations supplémentaires sur le plugin Wickr ATAK

Installez et associez le plugin Wickr pour ATAK

L'Android Team Awareness Kit (ATAK) est une solution Android utilisée par les agences militaires, étatiques et gouvernementales américaines qui ont besoin de capacités de connaissance de la situation pour la planification, l'exécution et la réponse aux incidents des missions. ATAK possède une architecture de plugins qui permet aux développeurs d'ajouter des fonctionnalités. Il permet aux utilisateurs de naviguer à l'aide du GPS et de données cartographiques géospatiales superposées à une connaissance situationnelle en temps réel des événements en cours. Dans ce document, nous vous montrons comment installer le plugin Wickr pour ATAK sur un appareil Android et le coupler avec le client Wickr. Cela vous permet d'envoyer des messages et de collaborer sur Wickr sans quitter l'application ATAK.

Installez le plugin Wickr pour ATAK

Suivez la procédure ci-dessous pour installer le plugin Wickr pour ATAK sur un appareil Android.

1. Accédez au Google Play Store et installez le plugin Wickr pour ATAK.
2. Ouvrez l'application ATAK sur votre appareil Android.
3. Dans l'application ATAK, choisissez l'icône du menu
   ()
   en haut à droite de l'écran, puis choisissez Plugins.
4. Choisissez Importer.
5. Dans la fenêtre contextuelle Select Import Type, choisissez Local SD et accédez à l'endroit où vous avez enregistré le plugin Wickr pour le fichier .apk ATAK.
6. Choisissez le fichier du plugin et suivez les instructions pour l'installer.

   > **Note**
   >
   > Si vous êtes invité à envoyer le fichier du plug-in pour analyse, choisissez Non.

7. L'application ATAK vous demandera si vous souhaitez charger le plugin. Choisissez OK.

Le plugin Wickr pour ATAK est maintenant installé. Passez à la section suivante Associer ATAK à Wickr pour terminer le processus.

Associez ATAK à Wickr

Effectuez la procédure suivante pour associer l'application ATAK à Wickr après avoir correctement installé le plugin Wickr pour ATAK.

1. Dans l'application ATAK, choisissez l'icône du menu
   ()
   en haut à droite de l'écran, puis choisissez Wickr Plugin.
2. Choisissez Pair Wickr.

   Une invite de notification apparaîtra vous demandant de vérifier les autorisations du plugin Wickr pour ATAK. Si l'invite de notification n'apparaît pas, ouvrez le client Wickr et accédez à Paramètres, puis à Applications connectées. Vous devriez voir le plugin dans la section En attente de l'écran.
3. Choisissez Approuver pour jumeler.
4. Choisissez le bouton Open Wickr ATAK Plugin pour revenir à l'application ATAK.

   Vous avez maintenant couplé avec succès le plugin ATAK et Wickr, et vous pouvez utiliser le plugin pour envoyer des messages et collaborer à l'aide de Wickr sans quitter l'application ATAK.

Dissocier le plugin Wickr pour ATAK

Vous pouvez dissocier le plugin Wickr pour ATAK.

Effectuez la procédure suivante pour dissocier le plugin ATAK de Wickr.

1. Dans l'application native, choisissez Paramètres, puis Applications connectées.
2. Sur l'écran Connected Apps, choisissez Wickr ATAK Plugin.
3. Sur l'écran du plugin Wickr ATAK, choisissez Supprimer en bas de l'écran.

   Vous venez de dissocier avec succès le plugin Wickr pour ATAK.

Composez et recevez un appel dans ATAK

Vous pouvez composer et recevoir un appel dans le plugin Wickr pour ATAK.

Procédez comme suit pour composer un numéro et recevoir un appel.

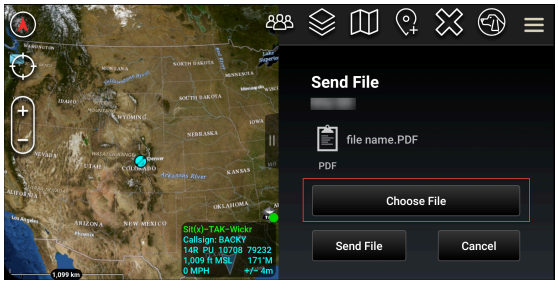
1. Ouvrez une fenêtre de discussion.
2. Dans la vue Carte, choisissez l'icône de l'utilisateur que vous souhaitez appeler.
3. Choisissez l'icône du téléphone en haut à droite de l'écran.
4. Une fois connecté, vous pouvez revenir à la vue du plugin ATAK et recevoir un appel.

Envoyer un fichier dans ATAK

Vous pouvez envoyer un fichier dans le plugin Wickr pour ATAK.

Pour envoyer un fichier, procédez comme suit.

1. Ouvrez une fenêtre de discussion.
2. Dans la vue Carte, recherchez l'utilisateur auquel vous souhaitez envoyer un fichier.
3. Lorsque vous trouvez l'utilisateur auquel vous souhaitez envoyer un fichier, sélectionnez son nom.
4. Sur l'écran Envoyer un fichier, sélectionnez Choisir un fichier, puis accédez au fichier que vous souhaitez envoyer.



5. Dans la fenêtre du navigateur, sélectionnez le fichier souhaité.
6. Sur l'écran Envoyer un fichier, choisissez Envoyer un fichier.

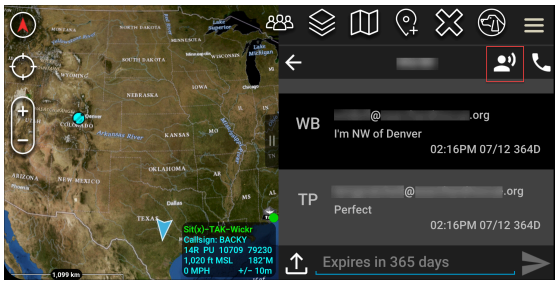
   L'icône de téléchargement s'affiche, indiquant que le fichier sélectionné est en cours de téléchargement.

Envoyer un message vocal sécurisé (Push-to-talk) dans ATAK

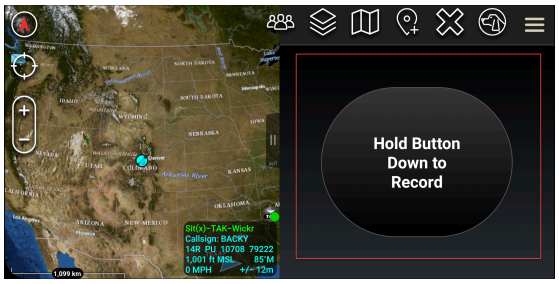
Vous pouvez envoyer un message vocal sécurisé (Push-to-talk) dans le plugin Wickr pour ATAK.

Procédez comme suit pour envoyer un message vocal sécurisé.

1. Ouvrez une fenêtre de discussion.
2. Choisissez l' Push-to-Talkicône en haut de l'écran, indiquée par l'icône représentant une personne en train de parler.



3. Sélectionnez le bouton Maintenir enfoncé pour enregistrer et maintenez-le enfoncé.



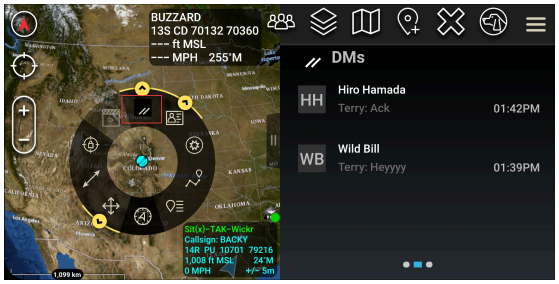
4. Enregistrez votre message.
5. Après avoir enregistré votre message, relâchez le bouton pour l'envoyer.

Pinwheel (accès rapide) pour ATAK

Le moulinet ou fonction d'accès rapide est utilisé pour les one-one-one conversations ou les messages directs.

Pour utiliser le moulinet, procédez comme suit.

1. Ouvrez simultanément la vue en écran partagé de la carte ATAK et du plugin Wickr for ATAK. La carte affiche vos coéquipiers ou vos actifs sur la vue cartographique.
2. Cliquez sur l'icône de l'utilisateur pour ouvrir le moulinet.
3. Cliquez sur l'icône Wickr pour afficher les options disponibles pour l'utilisateur sélectionné.

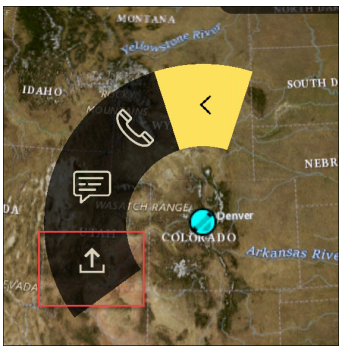


4. Sur le moulinet, choisissez l'une des icônes suivantes :

   - Téléphone : Choisissez d'appeler.

   - Message : Choisissez de discuter.

   - Envoyer un fichier : choisissez d'envoyer un fichier.



Navigation pour ATAK

L'interface utilisateur du plugin contient trois vues du plugin qui sont indiquées par les formes bleues et blanches en bas à droite de l'écran. Balayez vers la gauche ou vers la droite pour naviguer entre les vues.

- Affichage des contacts : créez un groupe de messages directs ou une conversation de salon.
- DMs affichage : Créez une one-to-one conversation. La fonctionnalité de chat fonctionne comme dans l'application native Wickr. Cette fonctionnalité vous permet de rester dans la vue Carte et de communiquer avec les autres utilisateurs du plugin.
- Vue des chambres : les pièces existantes de l'application native sont transférées. Tout ce qui est fait dans le plugin se reflète dans l'application native Wickr.

> **Note**
>
> Certaines fonctions, telles que la suppression d'une pièce, ne peuvent être exécutées que dans l'application native et en personne afin d'éviter toute modification involontaire par les utilisateurs et les interférences causées par l'équipement de terrain.

Liste des ports et domaines à autoriser pour votre réseau Wickr

Autoriser la liste des ports suivants pour garantir le bon fonctionnement de Wickr :

Ports

- Port TCP 443 (pour les messages et les pièces jointes)
- Ports UDP 16384-16584 (pour les appels)

Liste des domaines et adresses à autoriser par région

Si vous devez autoriser la liste de tous les domaines d'appel et adresses IP de serveurs possibles, consultez la liste suivante des domaines potentiels CIDRs par région. Consultez régulièrement cette liste, car elle est sujette à modification.

> **Note**
>
> Les e-mails d'inscription et de vérification sont envoyés depuis `no-reply@amazonaws.com` et`donotreply@wickr.email`.

USA Est (Virginie du Nord)

Domaines :	• gw-pro-prod.wickr.com • api.messaging. wickr.us-east-1.amazonaws.com • ingress.prod.calling.wickr.com
Appeler des adresses CIDR :	• 44,211,195,0/27 • 44,213,83,32/28
Adresses IP d'appel :	• 44,211,195,0 • 44,211,195,1 • 44,211,195,2 • 44,211,195,3 • 44,211,195,4 • 44,211,195,5 • 44,211,195,6 • 44,211,1195,7 • 44,211,195,8 • 44,211,195,9 • 44,211,195,10 • 44,211,195,11 • 44,211,195,12 • 44,211,195,13 • 44,211,195,14 • 44,211,195,15 • 44,211,195,16

- 44,211,195,17
- 44,211,195,18
- 44,211,195,19
- 44,211,195,20
- 44,211,195,21
- 44,211,195,22
- 44,211,195,23
- 44,211,195,24
- 44,211,195,25
- 44,211,195,26
- 44,211,195,27
- 44,211,195,28
- 44,211,195,29
- 44,211,195,30
- 44,211,195,31
- 44,213,83,32
- 44,213,83,33
- 44,213,83,34
- 44,213,83,35
- 44,213,83,36
- 44,213,83,37
- 44,213,83,38
- 44,213,83,39
- 44,213,83,40
- 44,213,83,41
- 44,213,83,42
- 44,213,83,43
- 44,213,83,44
- 44,213,83,45
- 44,213,83,46

	• 44,213,83,47

Asie-Pacifique (Malaisie)

Domaines :	• gw-pro-prod.wickr.com • api.messaging. wickr.ap-southeast-5.amazonaws.com • ingress.prod.calling. wickr.ap-southeast-5.amazonaws.com
Appeler des adresses CIDR :	• 43,216,226,160/28
Adresses IP d'appel :	• 43,216,226,160 • 43,216,226,161 • 43,216,226,162 • 43,216,226,163 • 43,216,226,164 • 43,216,226,165 • 43,216,226,166 • 43,216,226,167 • 43,216,226,168 • 43,216,226,169 • 43,216,226,170 • 43,216,226,171 • 43,216,226,172 • 43,216,226,173 • 43,216,226,174 • 43,216,226,175

Asie-Pacifique (Singapour)

Domaine :	• gw-pro-prod.wickr.com

	• api.messaging. wickr.ap-southeast-1.amazonaws.com • ingress.prod.calling. wickr.ap-southeast-1.amazonaws.com
Appeler des adresses CIDR :	• 47,129,23,144/28
Adresses IP d'appel :	• 47,129,23,144 • 47,129,23,145 • 47,129,23,146 • 47,129,23,147 • 47,129,23,148 • 47,129,23,149 • 47,129,23,150 • 47,129,23,151 • 47,129,23,152 • 47,129,23,153 • 47,129,23,154 • 47,129,23,155 • 47,129,23,156 • 47,129,23,157 • 47,129,23,158 • 47,129,23,159

Asie-Pacifique (Sydney)

Domaine :	• gw-pro-prod.wickr.com • api.messaging. wickr.ap-southeast-2.amazonaws.com • ingress.prod.calling. wickr.ap-southeast-2.amazonaws.com
Appeler des adresses CIDR :	• 3,27,180,208/28

Adresses IP d'appel :	• 3,27,180,208 • 3,27,180,209 • 3,27,180,210 • 3,27,180,211 • 3,27,180,212 • 3,27,180,213 • 3,27,180,214 • 3,27,180,215 • 3,27,180,216 • 3,27,180,217 • 3,27,180,218 • 3,27,180,219 • 3,27,180,220 • 3,27,180,221 • 3,27,180,222 • 3,27,180,223

Asie-Pacifique (Tokyo)

Domaine :	• gw-pro-prod.wickr.com • api.messaging. wickr.ap-northeast-1.amazonaws.com • ingress.prod.calling. wickr.ap-northeast-1.amazonaws.com
Appeler des adresses CIDR :	• 57,181,142,240/28
Adresses IP d'appel :	• 57,181,142,240 • 57,181,142,241 • 57,181,142,242 • 57,181,142,243 • 57,181,142,244

	• 57,181,142,245 • 57,181,142,246 • 57,181,142,247 • 57,181,142,248 • 57,181,142,249 • 57,181,142,250 • 57,181,142,251 • 57,181,142,252 • 57,181,142,253 • 57,181,142,254 • 57,181,142,255

Canada (Centre)

Domaine :	• gw-pro-prod.wickr.com • api.messaging. wickr.ca-central-1.amazonaws.com • ingress.prod.calling. wickr.ca-central-1.amazonaws.com
Appeler des adresses CIDR :	• 15,156,152,96/28
Adresses IP d'appel :	• 15,156,152,96 • 15,156,152,97 • 15,156,152,98 • 15,156,152,99 • 15,156,152,100 • 15,156,152,101 • 15,156,152,102 • 15,156,152,103 • 15,156,152,104 • 15,156,152,105

	• 15,156,152,106 • 15,156,152,107 • 15,156,152,108 • 15,156,152,109 • 15,156,152,110 • 15,156,152,111

Europe (Francfort)

Domaine :	• gw-pro-prod.wickr.com • api.messaging. wickr.eu-central-1.amazonaws.com • ingress.prod.calling. wickr.eu-central-1.amazonaws.com
Appeler des adresses CIDR :	• 3,78,252,32/28
Adresses IP d'appel :	• 3,78,252,32 • 3,78,252,33 • 3,78,252,34 • 3,78,252,35 • 3,78,252,36 • 3,78,252,37 • 3,78,252,38 • 3,78,252,39 • 3,78,252,40 • 3,78,252,41 • 3,78,252,42 • 3,78,252,43 • 3,78,252,44 • 3,78,252,45 • 3,78,252,46

	• 3,78,252,47
Adresses IP de messagerie :	• 3,163,236,183 • 3,163,238,183 • 3,163,251,183 • 3,163,232,183 • 3,163,241,183 • 3,163,245,183 • 3,163,248,183 • 3,163,234,183 • 3,163,237,183 • 3,163,243,183 • 3,163,247,183 • 3,163,240,183 • 3,163,242,183 • 3,163,244,183 • 3,163,246,183 • 3,163,249,183 • 3,163,252,183 • 3,163,235,183 • 3,163,250,183 • 3,163,239,183 • 3,163,233,183

Europe (Londres)

Domaine :	• gw-pro-prod.wickr.com • api.messaging. wickr.eu-west-2.amazonaws.com • ingress.prod.calling. wickr.eu-west-2.amazonaws.com

Appeler des adresses CIDR :	• 13,43,91,48/28
Adresses IP d'appel :	• 13,43,91,48 • 13,43,91,49 • 13,43,91,50 • 13,43,91,51 • 13,43,91,52 • 13,43,91,53 • 13,43,91,54 • 13,43,91,55 • 13,43,91,56 • 13,43,91,57 • 13,43,91,58 • 13,43,91,59 • 13,43,91,60 • 13,43,91,61 • 13,43,91,62 • 13,43,91,63

Europe (Stockholm)

Domaine :	• gw-pro-prod.wickr.com • api.messaging. wickr.eu-north-1.amazonaws.com • ingress.prod.calling. wickr.eu-north-1.amazonaws.com
Appeler des adresses CIDR :	• 13,60,164/28
Adresses IP d'appel :	• 13,60,164 • 13,601,65 • 13,601,66

	• 13,601,67 • 13,601,68 • 13,601,69 • 13,601,70 • 13,601,71 • 13,601,72 • 13,601,73 • 13,601,74 • 13,601,75 • 13,60,176 • 13,601,77 • 13,601,78 • 13,601,79

Europe (Zurich)

Domaine :	• gw-pro-prod.wickr.com • api.messaging. wickr.eu-central-2.amazonaws.com • ingress.prod.calling. wickr.eu-central-2 .amazonaws.com
Appeler des adresses CIDR :	• 16,63.106,224/28
Adresses IP d'appel :	• 16,63.106,224 • 16,63106,225 • 16,63.106,226 • 16,63.106,227 • 16,63.106,228 • 16,63106,229 • 16,63,106,230 • 16,63.106,231

	• 16,63.106,232 • 16,63.106,233 • 16,63.106,234 • 16,63.106,235 • 16,63.106,236 • 16,63.106,237 • 16,63.106,238 • 16,63.106,239

AWS GovCloud (US-Ouest)

Domaine :	• gw-pro-prod.wickr.com • api.messaging.wickr. us-gov-west-1. amazonaws.com • ingress-prod-calling.osier. us-gov-west-1. amazonaws.com • s3. us-gov-west-1. amazonaws.com • S-3 conseils. us-gov-west-1. amazonaws .com • s3.amazonaws.com • inscrivez-vous.wickr. us-gov-west-1. amazonaws.com • admin.wickr. us-gov-west-1. amazonaws.com • admin.messaging.wickr. us-gov-west-1. amazonaws.com • identité cognitive. us-gov-west-1. amazonaws .com • kinesis. us-gov-west-1. amazonaws.com
Appeler des adresses CIDR :	• 3,30,186,208/28 • 3,31.11.216/29
Adresses IP d'appel :	• 3,30,186,208

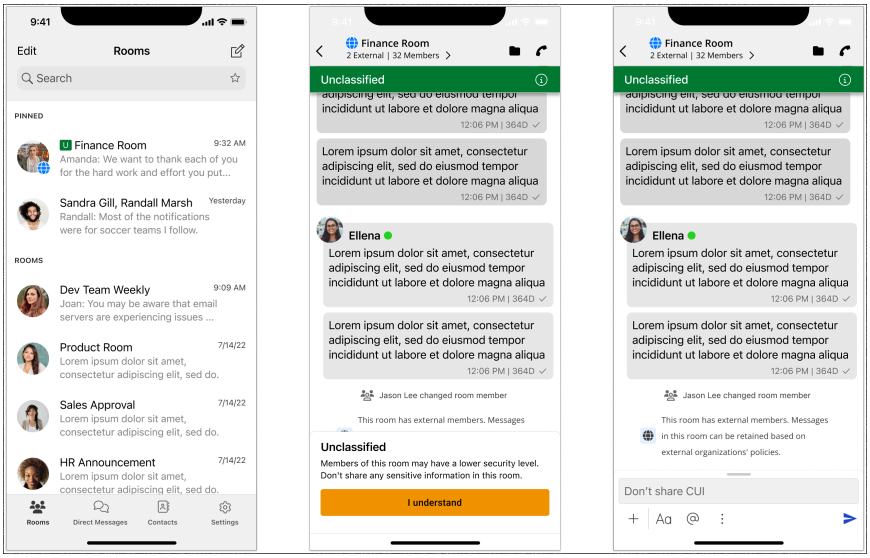
	• 3,30,186,209 • 3,30,186,210 • 3,30,186,211 • 3,30,186,212 • 3,30,186,213 • 3,30,186,214 • 3,30,186,215 • 3,30,186,216 • 3,30,186,217 • 3,30,186,218 • 3,30,186,219 • 3,30,186,220 • 3,30,186,221 • 3,30,186,222 • 3,30,186,223 • 3,311,1216 • 3,31.11.217 • 3,31.11.218 • 3,311,1219 • 3,311,1220 • 3,31.11.221 • 3,31.11.222 • 3,31.11.223

GovCloud classification et fédération transfrontalières

AWS Wickr propose un WickrGov client adapté aux GovCloud utilisateurs. La GovCloud Fédération permet la communication entre les GovCloud utilisateurs et les utilisateurs commerciaux. La fonction de classification transfrontalière permet de modifier l'interface utilisateur dans les conversations des GovCloud utilisateurs. En tant qu' GovCloud utilisateur, vous devez respecter des directives strictes concernant la classification définie par le gouvernement. Lorsque GovCloud les utilisateurs engagent

des conversations avec des utilisateurs commerciaux (utilisateurs Enterprise, AWS Wickr, utilisateurs invités), les avertissements non classifiés suivants s'affichent :

- Un tag U dans la liste des chambres
- Un accusé de réception non classifié sur l'écran du message
- Une bannière non classifiée au-dessus de la conversation



> **Note**
>
> Ces avertissements ne seront affichés que lorsqu'un GovCloud utilisateur est en conversation ou fait partie d'une salle avec des utilisateurs externes. Ils disparaîtront si les utilisateurs externes quittent la conversation. Aucun avertissement ne sera affiché dans les conversations entre GovCloud utilisateurs.

Aperçu du fichier pour AWS Wickr

Organisations utilisant le niveau Wickr Premium (y compris l'essai gratuit Premium) peuvent désormais gérer les autorisations de téléchargement de fichiers au niveau du groupe de sécurité.

Les téléchargements de fichiers sont activés par défaut dans les groupes de sécurité. Les administrateurs peuvent activer ou désactiver le téléchargement de fichiers via le panneau d'administration. Ce paramètre est appliqué à l'ensemble du réseau Wickr.

Pour activer ou désactiver le téléchargement de fichiers, procédez comme suit.

1. Ouvrez le AWS Management Console pour Wickr à l'adresse https://console.aws.amazon.com/wickr/.
2. Sur la page Réseaux, sélectionnez le nom du réseau pour accéder à ce réseau.
3. Dans le panneau de navigation, choisissez Groupes de sécurité.
4. Sélectionnez le nom du groupe de sécurité que vous souhaitez modifier.

   La page des détails du groupe de sécurité affiche les paramètres du groupe de sécurité dans différents onglets.
5. Sous l'onglet Messagerie, dans la section Médias et liens, choisissez Modifier.
6. Sur la page Modifier le contenu multimédia et les liens, cochez ou décochez l'option Téléchargement de fichiers.
7. Sélectionnez Enregistrer les modifications.

Lorsque le téléchargement de fichiers est activé pour un groupe de sécurité, les utilisateurs peuvent télécharger des fichiers partagés dans des messages directs et dans des salles. Si les téléchargements sont désactivés, ils peuvent uniquement prévisualiser ces fichiers et les télécharger dans l'onglet Fichiers, mais ne peuvent pas les télécharger. Il est également interdit aux utilisateurs de prendre des captures d'écran ; les tentatives entraîneront un écran noir.

> **Note**
>
> Lorsque les téléchargements de fichiers sont désactivés, tous les utilisateurs de ce groupe de sécurité doivent utiliser les versions 6.54 ou supérieures de Wickr pour que ce paramètre de fichier s'applique.

> **Note**
>
> Dans les salles où sont présents des utilisateurs de différents réseaux (en raison de la fédération) et de groupes de sécurité, la capacité de chaque utilisateur à prévisualiser ou à télécharger des fichiers dépend des paramètres spécifiques de son groupe de sécurité. Par conséquent, certains utilisateurs peuvent télécharger des fichiers dans une pièce tandis que d'autres peuvent uniquement les prévisualiser.

Gérer les utilisateurs dans AWS Wickr

Dans la section Gestion des utilisateurs de AWS Management Console for Wickr, vous pouvez voir les utilisateurs et les robots actuels de Wickr, et modifier leurs informations.

Rubriques

Répertoire des équipes dans le réseau AWS Wickr

Vous pouvez consulter les utilisateurs actuels de Wickr et modifier leurs informations dans la section Gestion des utilisateurs de AWS Management Console for Wickr.

Rubriques

Afficher les utilisateurs du réseau AWS Wickr

Vous pouvez consulter les détails des utilisateurs enregistrés sur votre réseau Wickr.

Suivez la procédure suivante pour voir les utilisateurs enregistrés sur votre réseau Wickr.

1. Ouvrez le AWS Management Console pour Wickr à l'adresse https://console.aws.amazon.com/wickr/.
2. Sur la page Réseaux, sélectionnez le nom du réseau pour accéder à ce réseau.
3. Dans le volet de navigation, sélectionnez Gestion des utilisateurs.

   L'onglet Répertoire de l'équipe affiche les utilisateurs enregistrés sur votre réseau Wickr, y compris leur nom, leur adresse e-mail, le groupe de sécurité attribué et leur statut actuel. Pour

les utilisateurs actuels, vous pouvez consulter leurs appareils, modifier leurs informations, les suspendre, les supprimer et les transférer vers un autre réseau Wickr.

Inviter un utilisateur dans le réseau AWS Wickr

Vous pouvez inviter un utilisateur dans votre réseau Wickr.

Complétez la procédure suivante pour inviter un utilisateur dans votre réseau Wickr.

1. Ouvrez le AWS Management Console pour Wickr à l'adresse https://console.aws.amazon.com/wickr/.
2. Sur la page Réseaux, sélectionnez le nom du réseau pour accéder à ce réseau.
3. Dans le volet de navigation, sélectionnez Gestion des utilisateurs.
4. Dans l'onglet Répertoire de l'équipe, choisissez Inviter un utilisateur.
5. Sur la page Inviter un utilisateur, entrez l'adresse e-mail et le groupe de sécurité de l'utilisateur. L'adresse e-mail et le groupe de sécurité sont les seuls champs obligatoires. Assurez-vous de choisir le groupe de sécurité approprié pour l'utilisateur. Wickr enverra un e-mail d'invitation à l'adresse que vous avez spécifiée pour l'utilisateur.
6. Choisissez Invite user.

   Un e-mail est envoyé à l'utilisateur. L'e-mail fournit des liens de téléchargement pour les applications clientes Wickr, ainsi qu'un lien pour s'inscrire à Wickr. Lorsque les utilisateurs s'inscrivent à Wickr en utilisant le lien contenu dans l'e-mail, leur statut dans le répertoire de l'équipe Wickr passe de En attente à Actif.

Modifier les utilisateurs dans le réseau AWS Wickr

Vous pouvez modifier les utilisateurs de votre réseau Wickr.

Suivez la procédure ci-dessous pour modifier un utilisateur.

1. Ouvrez le AWS Management Console pour Wickr à l'adresse https://console.aws.amazon.com/wickr/.
2. Sur la page Réseaux, sélectionnez le nom du réseau pour accéder à ce réseau.
3. Dans le volet de navigation, sélectionnez Gestion des utilisateurs.

4. Dans l'onglet Répertoire de l'équipe, sélectionnez l'icône représentant des points de suspension verticaux (trois points) de l'utilisateur que vous souhaitez modifier.
5. Choisissez Modifier.
6. Modifiez les informations utilisateur, puis choisissez Enregistrer les modifications.

Supprimer un utilisateur dans le réseau AWS Wickr

Vous pouvez supprimer un utilisateur de votre réseau Wickr.

Pour supprimer un utilisateur, procédez comme suit.

1. Ouvrez le AWS Management Console pour Wickr à l'adresse https://console.aws.amazon.com/wickr/.
2. Sur la page Réseaux, sélectionnez le nom du réseau pour accéder à ce réseau.
3. Dans le volet de navigation, sélectionnez Gestion des utilisateurs.
4. Dans l'onglet Répertoire de l'équipe, sélectionnez l'icône représentant des points de suspension verticaux (trois points) de l'utilisateur que vous souhaitez supprimer.
5. Choisissez Supprimer pour supprimer l'utilisateur.

   Lorsque vous supprimez un utilisateur, celui-ci n'est plus en mesure de se connecter à votre réseau Wickr dans le client Wickr.
6. Dans la fenêtre contextuelle, choisissez Supprimer.

Supprimer en bloc des utilisateurs dans le réseau AWS Wickr

Vous pouvez supprimer en bloc les utilisateurs du réseau Wickr dans la section Gestion des utilisateurs de AWS Management Console Wickr.

> **Note**
>
> L'option de suppression groupée d'utilisateurs ne s'applique que lorsque l'authentification unique n'est pas activée.

Pour supprimer en bloc les utilisateurs de votre réseau Wickr à l'aide d'un modèle CSV, procédez comme suit.

1. Ouvrez le AWS Management Console pour Wickr à l'adresse https://console.aws.amazon.com/wickr/.
2. Sur la page Réseaux, sélectionnez le nom du réseau pour accéder à ce réseau.
3. Dans le volet de navigation, sélectionnez Gestion des utilisateurs.
4. L'onglet Répertoire des équipes affiche les utilisateurs enregistrés sur votre réseau Wickr.
5. Dans l'onglet Annuaire de l'équipe, choisissez Gérer les utilisateurs, puis choisissez Supprimer en bloc.
6. Sur la page Supprimer des utilisateurs en bloc, téléchargez l'exemple de modèle CSV. Pour télécharger le modèle d'exemple, choisissez Télécharger le modèle.
7. Complétez le modèle en ajoutant l'adresse e-mail des utilisateurs que vous souhaitez supprimer en bloc de votre réseau.
8. Téléchargez le modèle CSV complété. Vous pouvez glisser-déposer le fichier dans la zone de téléchargement ou sélectionner Choisir un fichier.
9. Cochez la case, je comprends que la suppression d'un utilisateur n'est pas réversible.
10. Choisissez Supprimer les utilisateurs.

> **Note**
>
> Cette action commencera immédiatement à supprimer des utilisateurs et peut prendre plusieurs minutes. Les utilisateurs supprimés ne pourront plus se connecter à votre réseau Wickr dans le client Wickr.

Pour supprimer en bloc les utilisateurs de votre réseau Wickr en téléchargeant un fichier CSV du répertoire de votre équipe, procédez comme suit.

1. Ouvrez le AWS Management Console pour Wickr à l'adresse https://console.aws.amazon.com/wickr/.
2. Sur la page Réseaux, sélectionnez le nom du réseau pour accéder à ce réseau.
3. Dans le volet de navigation, sélectionnez Gestion des utilisateurs.
4. L'onglet Répertoire des équipes affiche les utilisateurs enregistrés sur votre réseau Wickr.
5. Dans l'onglet Répertoire de l'équipe, choisissez Gérer les utilisateurs, puis sélectionnez Télécharger au format CSV.

6. Après avoir téléchargé le modèle CSV de répertoire d'équipe, supprimez les lignes d'utilisateurs qui n'ont pas besoin d'être supprimées.
7. Dans l'onglet Annuaire de l'équipe, choisissez Gérer les utilisateurs, puis choisissez Supprimer en bloc.
8. Sur la page Supprimer des utilisateurs en bloc, téléchargez le modèle CSV du répertoire d'équipe. Vous pouvez glisser-déposer le fichier dans la zone de téléchargement ou sélectionner Choisir un fichier.
9. Cochez la case, je comprends que la suppression d'un utilisateur n'est pas réversible.
10. Choisissez Supprimer les utilisateurs.

> **Note**
>
> Cette action commencera immédiatement à supprimer des utilisateurs et peut prendre plusieurs minutes. Les utilisateurs supprimés ne pourront plus se connecter à votre réseau Wickr dans le client Wickr.

Suspension groupée d'utilisateurs dans le réseau AWS Wickr

Vous pouvez suspendre en bloc les utilisateurs du réseau Wickr dans la section Gestion des utilisateurs de AWS Management Console Wickr.

> **Note**
>
> L'option de suspension groupée des utilisateurs ne s'applique que lorsque l'authentification unique n'est pas activée.

Pour suspendre en bloc les utilisateurs de votre réseau Wickr, procédez comme suit.

1. Ouvrez le AWS Management Console pour Wickr à l'adresse https://console.aws.amazon.com/wickr/.
2. Sur la page Réseaux, sélectionnez le nom du réseau pour accéder à ce réseau.
3. Dans le volet de navigation, sélectionnez Gestion des utilisateurs.
4. L'onglet Répertoire des équipes affiche les utilisateurs enregistrés sur votre réseau Wickr.

5. Dans l'onglet Annuaire de l'équipe, choisissez Gérer les utilisateurs, puis choisissez Suspension groupée.
6. Sur la page Suspension groupée des utilisateurs, téléchargez l'exemple de modèle CSV. Pour télécharger le modèle d'exemple, choisissez Télécharger le modèle.
7. Complétez le modèle en ajoutant l'adresse e-mail des utilisateurs que vous souhaitez suspendre en bloc de votre réseau.
8. Téléchargez le modèle CSV complété. Vous pouvez glisser-déposer le fichier dans la zone de téléchargement ou sélectionner Choisir un fichier.
9. Choisissez Suspendre les utilisateurs.

> **Note**
>
> Cette action commencera immédiatement à suspendre les utilisateurs et peut prendre plusieurs minutes. Les utilisateurs suspendus ne peuvent pas se connecter à votre réseau Wickr dans le client Wickr. Lorsque vous suspendez un utilisateur actuellement connecté à votre réseau Wickr dans le client, cet utilisateur est automatiquement déconnecté.

Utilisateurs invités du réseau AWS Wickr

La fonctionnalité utilisateur invité de Wickr permet aux utilisateurs invités individuels de se connecter au client Wickr et de collaborer avec les utilisateurs du réseau Wickr. Les administrateurs Wickr peuvent activer ou désactiver les utilisateurs invités pour leurs réseaux Wickr.

Une fois la fonctionnalité activée, les utilisateurs invités à rejoindre votre réseau Wickr peuvent interagir avec les utilisateurs de votre réseau Wickr. Des frais vous seront facturés Compte AWS pour la fonctionnalité d'utilisateur invité. Pour plus d'informations sur la tarification de la fonctionnalité utilisateur invité, consultez la page de tarification de Wickr sous Extensions de tarification.

Rubriques

- Activer ou désactiver les utilisateurs invités dans le réseau AWS Wickr
- Afficher le nombre d'utilisateurs invités dans le réseau AWS Wickr
- Afficher l'utilisation mensuelle dans le réseau AWS Wickr
- Afficher les utilisateurs invités dans le réseau AWS Wickr

- Bloquer un utilisateur invité dans le réseau AWS Wickr

Activer ou désactiver les utilisateurs invités dans le réseau AWS Wickr

Vous pouvez activer ou désactiver les utilisateurs invités dans votre réseau Wickr.

Suivez la procédure suivante pour activer ou désactiver les utilisateurs invités pour votre réseau Wickr.

1. Ouvrez le AWS Management Console pour Wickr à l'adresse https://console.aws.amazon.com/wickr/.
2. Sur la page Réseaux, sélectionnez le nom du réseau pour accéder à ce réseau.
3. Dans le panneau de navigation, choisissez Groupes de sécurité.
4. Sélectionnez le nom d'un groupe de sécurité spécifique.

   > **Note**
   >
   > Vous ne pouvez activer les utilisateurs invités que pour des groupes de sécurité individuels. Pour activer les utilisateurs invités pour tous les groupes de sécurité de votre réseau Wickr, vous devez activer la fonctionnalité pour chaque groupe de sécurité de votre réseau.

5. Choisissez l'onglet Fédération dans le groupe de sécurité.
6. L'option permettant d'activer les utilisateurs invités est disponible à deux endroits :

   - Fédération locale : pour les réseaux situés dans l'est des États-Unis (Virginie du Nord), choisissez Modifier dans la section Fédération locale de la page.
   - Fédération mondiale : pour tous les autres réseaux des autres régions, choisissez Modifier dans la section Fédération mondiale de la page.

7. Sur la page Modifier la fédération, sélectionnez Activer la fédération.
8. Choisissez Enregistrer les modifications pour enregistrer la modification et la rendre effective pour le groupe de sécurité.

   Les utilisateurs enregistrés dans le groupe de sécurité spécifique de votre réseau Wickr peuvent désormais interagir avec les utilisateurs invités. Pour plus d'informations, consultez la section Utilisateurs invités dans le guide de l'utilisateur de Wickr.

Afficher le nombre d'utilisateurs invités dans le réseau AWS Wickr

Vous pouvez consulter le nombre d'utilisateurs invités dans votre réseau Wickr.

Suivez la procédure suivante pour afficher le nombre d'utilisateurs invités pour votre réseau Wickr.

1. Ouvrez le AWS Management Console pour Wickr à l'adresse https://console.aws.amazon.com/wickr/.
2. Sur la page Réseaux, sélectionnez le nom du réseau pour accéder à ce réseau.
3. Dans le volet de navigation, sélectionnez Gestion des utilisateurs.

   La page de gestion des utilisateurs affiche le nombre d'utilisateurs invités dans votre réseau Wickr.

Afficher l'utilisation mensuelle dans le réseau AWS Wickr

Vous pouvez consulter le nombre d'utilisateurs invités avec lesquels votre réseau a communiqué au cours d'une période de facturation.

Suivez la procédure suivante pour consulter votre utilisation mensuelle de votre réseau Wickr.

1. Ouvrez le AWS Management Console pour Wickr à l'adresse https://console.aws.amazon.com/wickr/.
2. Sur la page Réseaux, sélectionnez le nom du réseau pour accéder à ce réseau.
3. Dans le volet de navigation, sélectionnez Gestion des utilisateurs.
4. Sélectionnez l'onglet Utilisateurs invités.

   L'onglet Utilisateurs invités affiche l'utilisation mensuelle des utilisateurs invités.

   > **Note**
   >
   > Les données de facturation des clients sont mises à jour toutes les 24 heures.

Afficher les utilisateurs invités dans le réseau AWS Wickr

Vous pouvez consulter les utilisateurs invités avec lesquels un utilisateur du réseau a communiqué au cours d'une période de facturation spécifique.

Suivez la procédure ci-dessous pour voir les utilisateurs invités avec lesquels un utilisateur du réseau a communiqué au cours d'une période de facturation spécifique.

1. Ouvrez le AWS Management Console pour Wickr à l'adresse https://console.aws.amazon.com/wickr/.
2. Sur la page Réseaux, sélectionnez le nom du réseau pour accéder à ce réseau.
3. Dans le volet de navigation, sélectionnez Gestion des utilisateurs.
4. Sélectionnez l'onglet Utilisateurs invités.

   L'onglet Utilisateurs invités affiche les utilisateurs invités de votre réseau.

Bloquer un utilisateur invité dans le réseau AWS Wickr

Vous pouvez bloquer et débloquer un utilisateur invité dans votre réseau Wickr. Les utilisateurs bloqués ne peuvent communiquer avec aucun membre de votre réseau.

Pour bloquer un utilisateur invité

1. Ouvrez le AWS Management Console pour Wickr à l'adresse https://console.aws.amazon.com/wickr/.
2. Sur la page Réseaux, sélectionnez le nom du réseau pour accéder à ce réseau.
3. Dans le volet de navigation, sélectionnez Gestion des utilisateurs.
4. Sélectionnez l'onglet Utilisateurs invités.

   L'onglet Utilisateurs invités affiche les utilisateurs invités de votre réseau.
5. Dans la section Utilisateurs invités, recherchez l'adresse e-mail de l'utilisateur invité que vous souhaitez bloquer.
6. Sur le côté droit du nom de l'utilisateur invité, sélectionnez les trois points, puis choisissez Bloquer l'utilisateur invité.
7. Choisissez Bloquer dans la fenêtre contextuelle.
8. Pour afficher la liste des utilisateurs bloqués sur votre réseau Wickr, sélectionnez le menu déroulant État, puis sélectionnez Bloqué.

Pour débloquer un utilisateur invité

1. Ouvrez le AWS Management Console pour Wickr à l'adresse https://console.aws.amazon.com/wickr/.
2. Sur la page Réseaux, sélectionnez le nom du réseau pour accéder à ce réseau.
3. Dans le volet de navigation, sélectionnez Gestion des utilisateurs.
4. Sélectionnez l'onglet Utilisateurs invités.

   L'onglet Utilisateurs invités affiche les utilisateurs invités de votre réseau.
5. Sélectionnez le menu déroulant État, puis sélectionnez Bloqué.
6. Dans la section Bloqué, recherchez l'e-mail de l'utilisateur invité que vous souhaitez débloquer.
7. Sur le côté droit du nom de l'utilisateur invité, sélectionnez les trois points, puis choisissez Débloquer l'utilisateur.
8. Choisissez Débloquer dans la fenêtre contextuelle.

Sécurité dans AWS Wickr

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 ceci 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 Wickr, consultez la section 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 Wickr. Les rubriques suivantes vous montrent comment configurer Wickr pour répondre à vos objectifs de sécurité et de conformité. Vous apprenez également à utiliser d'autres AWS services qui vous aident à surveiller et à sécuriser vos ressources Wickr.

Rubriques

Protection des données dans AWS Wickr

Le modèle de responsabilité AWS partagée Le modèle s'applique à la protection des données dans AWS Wickr. 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 d'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 Gestion des identités et des accès AWS (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 Wickr ou un autre utilisateur 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.

Gestion des identités et des accès pour AWS Wickr

Gestion des identités et des accès AWS (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 Wickr. IAM est un Service AWS outil que vous pouvez utiliser sans frais supplémentaires.

Rubriques

Audience d'AWS Wickr

La façon dont vous utilisez Gestion des identités et des accès AWS (IAM) varie en fonction de votre rôle :

- Utilisateur du service : demandez des autorisations à votre administrateur si vous ne pouvez pas accéder aux fonctionnalités (voir Résolution des problèmes d'identité et d'accès à AWS Wickr)
- Administrateur du service : déterminez l’accès des utilisateurs et soumettez les demandes d’autorisation (voir Comment AWS Wickr fonctionne avec IAM)
- Administrateur IAM : rédigez des politiques pour gérer l’accès (voir Exemples de politiques basées sur l'identité pour AWS Wickr)

Authentification avec des identités pour AWS Wickr

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

Vous pouvez vous connecter en tant qu'identité fédérée à l'aide d'informations d'identification provenant d'une source d'identité telle que AWS IAM Identity Center (IAM Identity Center), d'une authentification unique ou d'informations d'identification. Google/Facebook Pour plus d'informations sur la connexion, consultez Connexion à votre Compte AWS dans le Guide de l'utilisateur Connexion à AWS .

Pour l'accès par programmation, AWS fournit un SDK et une CLI pour signer les demandes de manière cryptographique. Pour plus d'informations, consultez Signature AWS Version 4 pour les demandes d'API dans le Guide de l'utilisateur IAM.

Compte AWS utilisateur root

Lorsque vous créez un Compte AWS, vous commencez par une seule identité de connexion appelée utilisateur Compte AWS root qui dispose d'un accès complet à toutes Services AWS les ressources. Il est vivement déconseillé d'utiliser l'utilisateur racine pour vos tâches quotidiennes. Pour les tâches qui requièrent des informations d'identification de l'utilisateur racine, consultez Tâches qui requièrent les informations d'identification de l'utilisateur racine dans le Guide de l'utilisateur IAM.

Identité fédérée

Il est recommandé d'obliger les utilisateurs humains à utiliser la fédération avec un fournisseur d'identité pour accéder à Services AWS l'aide d'informations d'identification temporaires.

Une identité fédérée est un utilisateur provenant de l'annuaire de votre entreprise, de votre fournisseur d'identité Web ou Directory Service qui y accède à Services AWS l'aide d'informations d'identification provenant d'une source d'identité. Les identités fédérées 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. Pour plus d'informations, 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 qui dispose d'autorisations spécifiques pour une seule personne ou application. Nous vous recommandons d'utiliser ces informations d'identification temporaires au lieu des utilisateurs IAM avec des informations d'identification à long terme. Pour plus d'informations, voir Exiger des utilisateurs humains qu'ils utilisent la fédération avec un fournisseur d'identité pour accéder à AWS l'aide d'informations d'identification temporaires dans le guide de l'utilisateur IAM.

Les groupes IAM spécifient une collection d'utilisateurs IAM et permettent de gérer plus facilement les autorisations pour de grands ensembles d'utilisateurs. 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 dotée d'autorisations spécifiques qui fournit des informations d'identification temporaires. Vous pouvez assumer un rôle en passant d'un rôle d'utilisateur à un rôle IAM (console) ou en appelant une opération d' AWS API AWS CLI ou d'API. Pour plus d'informations, consultez Méthodes pour endosser un rôle dans le Guide de l'utilisateur IAM.

Les rôles IAM sont utiles pour l'accès des utilisateurs fédérés, les autorisations temporaires des utilisateurs IAM, les accès intercompte, les accès entre services et les applications exécutées sur Amazon EC2. Pour plus d'informations, consultez Accès intercompte aux ressources dans IAM dans le Guide de l'utilisateur IAM.

Gestion de l'accès à l'aide de politiques pour AWS Wickr

Vous contrôlez l'accès en AWS créant des politiques et en les associant à AWS des identités ou à des ressources. Une politique définit les autorisations lorsqu'elles sont associées à une identité ou à une ressource. AWS évalue ces politiques lorsqu'un directeur fait une demande. La plupart des politiques sont stockées AWS sous forme de documents JSON. Pour plus d'informations les documents de politique JSON, consultez Vue d'ensemble des politiques JSON dans le Guide de l'utilisateur IAM.

À l'aide de politiques, les administrateurs précisent qui a accès à quoi en définissant 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. Un administrateur IAM crée des politiques IAM et les ajoute aux rôles, que les utilisateurs peuvent ensuite assumer. Les politiques IAM définissent les autorisations quelle que soit la méthode que vous utilisez pour exécuter l'opération.

Politiques basées sur l’identité

Les stratégies basées sur l’identité sont des documents de stratégie d’autorisations JSON que vous attachez à une identité (utilisateur, groupe ou rôle). Ces politiques contrôlent les actions que peuvent exécuter ces identités, 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 des politiques intégrées (intégrées directement dans une seule identité) ou des politiques gérées (politiques autonomes associées à plusieurs identités). Pour découvrir comment choisir entre des politiques gérées et 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. Les exemples incluent les politiques de confiance de rôle IAM et les stratégies de compartiment Amazon S3. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour contrôler l’accès à une ressource spécifique. Vous devez spécifier un principal dans une politique basée sur les ressources.

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 obtenues représentent la combinaison des politiques basées sur l'identité de l'entité et de ses limites d'autorisations. 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 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.

AWS politiques gérées pour AWS Wickr

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.

Services AWS maintenir et mettre 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.

AWS politique gérée : AWSWickr FullAccess

Vous pouvez associer la politique `AWSWickrFullAccess` à vos identités IAM. Cette politique accorde une autorisation administrative complète au service Wickr, y compris celle AWS Management Console pour Wickr dans le. AWS Management Console Pour plus d'informations sur l'attachement de politiques à une identité, consultez la section Ajouter et supprimer des autorisations d'identité IAM dans le Guide de l'Gestion des identités et des accès AWS utilisateur.

Détails de l'autorisation

Cette politique inclut les autorisations suivantes.

- `wickr`— Accorde une autorisation administrative complète au service Wickr.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "wickr:*",
            "Resource": "*"
        }
    ]
}
```

Mises à jour des politiques AWS gérées par Wickr

Consultez les détails des mises à jour des politiques AWS gérées pour Wickr 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 du document Wickr.

Modifier	Description	Date
AWSWickrFullAccess : nouvelle politique	Wickr a ajouté une nouvelle politique qui accorde des autorisations administratives complètes au service Wickr, y compris la console d'adminis tration Wickr dans le. AWS Management Console	28 novembre 2022
Wickr a commencé à suivre les modifications	Wickr a commencé à suivre les modifications apportées à ses politiques AWS gérées.	28 novembre 2022

Comment AWS Wickr fonctionne avec IAM

Avant d'utiliser IAM pour gérer l'accès à Wickr, découvrez quelles fonctionnalités IAM peuvent être utilisées avec Wickr.

Fonctionnalités IAM que vous pouvez utiliser avec AWS Wickr

Fonctionnalité IAM	Support en osier
Politiques basées sur l'identité	Oui
Politiques basées sur les ressources	Non
Actions de politique	Oui
Ressources de politique	Non
Clés de condition d'une politique	Non
ACLs	Non
ABAC (étiquettes dans les politiques)	Non
Informations d'identification temporaires	Non

Fonctionnalité IAM	Support en osier
Autorisations de principals	Non
Rôles du service	Non
Rôles liés à un service	Non

Pour obtenir une vue d'ensemble de la façon dont Wickr 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 Wickr

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. 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 Wickr

Pour voir des exemples de politiques basées sur l'identité de Wickr, consultez. Exemples de politiques basées sur l'identité pour AWS Wickr

Politiques basées sur les ressources au sein de Wickr

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. Pour plus d'informations, consultez Accès intercompte aux ressources dans IAM dans le Guide de l'utilisateur IAM.

Actions politiques pour Wickr

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

Pour consulter la liste des actions Wickr, consultez la section Actions définies par AWS Wickr dans le Service Authorization Reference.

Les actions politiques dans Wickr utilisent le préfixe suivant avant l'action :

```
wickr
```

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

```
"Action": [
      "wickr:action1",
      "wickr:action2"
         ]
```

Pour voir des exemples de politiques basées sur l'identité de Wickr, consultez. Exemples de politiques basées sur l'identité pour AWS Wickr

Ressources politiques pour Wickr

Prend en charge les ressources de politique : non

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. Il est recommandé de définir une ressource à l'aide de son Amazon Resource Name (ARN). Pour les actions qui ne sont pas compatibles avec les autorisations de niveau ressource, 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 Wickr et de leurs caractéristiques ARNs, consultez la section Ressources définies par AWS Wickr dans la référence d'autorisation de service. Pour savoir avec quelles actions vous pouvez spécifier l'ARN de chaque ressource, consultez Actions définies par AWS Wickr.

Pour voir des exemples de politiques basées sur l'identité de Wickr, consultez. Exemples de politiques basées sur l'identité pour AWS Wickr

Clés de conditions de politique pour Wickr

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

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` indique à quel moment les instructions s'exécutent en fonction de critères définis. 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. 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 Wickr, consultez la section Clés de condition pour AWS Wickr dans la référence d'autorisation de service. Pour savoir avec quelles actions et ressources vous pouvez utiliser une clé de condition, consultez Actions définies par AWS Wickr.

Pour voir des exemples de politiques basées sur l'identité de Wickr, consultez. Exemples de politiques basées sur l'identité pour AWS Wickr

ACLs à Wickr

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 Wickr

Prise en charge d'ABAC (balises dans les politiques) : non

Le contrôle d'accès par attributs (ABAC) est une stratégie d'autorisation qui définit les autorisations en fonction des attributs appelés balises. Vous pouvez associer des balises aux entités et aux AWS ressources IAM, puis concevoir des politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise de la ressource.

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.

Utiliser des informations d'identification temporaires avec Wickr

Supporte les informations d'identification temporaires : Non

Les informations d'identification temporaires fournissent un accès à court terme aux AWS ressources et sont automatiquement créées lorsque vous utilisez la fédération ou que vous changez de rôle. 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 et Services AWS compatibles avec IAM dans le Guide de l'utilisateur IAM.

Autorisations principales interservices pour Wickr

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

Les sessions d'accès direct (FAS) utilisent les autorisations du principal appelant et Service AWS, combinées Service AWS à la demande d'envoi de demandes aux services en aval. Pour plus de détails sur la politique relative à la transmission de demandes FAS, consultez la section Sessions de transmission d'accès.

Rôles de service pour Wickr

Prend en charge les rôles de service : Non

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 pour un rôle de service peut perturber les fonctionnalités de Wickr. Modifiez les rôles de service uniquement lorsque Wickr fournit des conseils pour le faire.

Rôles liés à un service pour Wickr

Prend en charge les rôles liés à un service : non

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 AWS Wickr

Par défaut, un nouvel utilisateur IAM ne dispose d'aucune autorisation. Un administrateur IAM doit créer et attribuer des politiques IAM qui autorisent les utilisateurs à administrer le service AWS Wickr. Un exemple de politique d'autorisation est exposé ci-dessous.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "wickr:CreateAdminSession",
                "wickr:ListNetworks"
            ],
            "Resource": "*"
        }
    ]
}
```

Cet exemple de politique autorise les utilisateurs à répertorier les réseaux Wickr à l'aide de AWS Management Console for Wickr. Pour en savoir plus sur les éléments d'un énoncé de politique IAM, consultez Politiques basées sur l'identité pour Wickr. Pour savoir comment créer une stratégie IAM à partir de ces exemples de documents de stratégie JSON, consultez Création de stratégies dans l'onglet JSON dans le Guide de l'utilisateur IAM.

Vous pouvez également créer une politique IAM pour permettre aux utilisateurs d'accéder à des actions d'API spécifiques. L'accès aux actions d'API est géré séparément de la console AWS Wickr. Vous trouverez ci-dessous un exemple de politique qui accorde un accès en lecture seule à des actions d'API spécifiques. Pour plus d'informations sur les actions d'API, consultez la section Bienvenue dans le guide de référence des API AWS Wickr.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid": "WickrAPIReadOnlyAccess",
            "Effect": "Allow",
            "Action": [
                "wickr:ListNetworks",
                "wickr:ListUsers",
                "wickr:GetNetworkSettings",
                "wickr:GetNetwork",
                "wickr:GetUser",
                "wickr:ListTagsForResource"
            ],
            "Resource": "*"
        }
    ]
}
```

Rubriques

- Bonnes pratiques en matière de politiques
- Utilisation du AWS Management Console for Wickr
- 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 les ressources Wickr de 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 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 du AWS Management Console for Wickr

Associez la politique `AWSWickrFullAccess` AWS gérée à vos identités IAM pour leur accorder des autorisations administratives complètes sur le service Wickr, y compris la console d'administration Wickr dans le. AWS Management Console Pour de plus amples informations, veuillez consulter AWS politique gérée : AWSWickr FullAccess.

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": "*"
        }
    ]
}
```

Résolution des problèmes d'identité et d'accès à AWS Wickr

Utilisez les informations suivantes pour vous aider à diagnostiquer et à résoudre les problèmes courants que vous pouvez rencontrer lorsque vous travaillez avec Wickr et IAM.

Rubriques

- Je ne suis pas autorisé à effectuer une action administrative dans le AWS Management Console for Wickr

Je ne suis pas autorisé à effectuer une action administrative dans le AWS Management Console for Wickr

Si le AWS Management Console for Wickr vous indique que vous n'êtes pas autorisé à effectuer une action, vous devez contacter votre administrateur pour obtenir de l'aide. Votre administrateur est la personne qui vous a fourni vos informations de connexion.

L'exemple d'erreur suivant se produit lorsque l'utilisateur `mateojackson` IAM essaie d'utiliser AWS Management Console for Wickr pour créer, gérer ou afficher des réseaux Wickr dans AWS Management Console for Wickr mais ne dispose pas des autorisations et. `wickr:CreateAdminSession` `wickr:ListNetworks`

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 wickr:ListNetworks
```

Dans ce cas, Mateo demande à son administrateur de mettre à jour ses politiques afin de lui permettre d'accéder à Wickr AWS Management Console à l'aide des actions `wickr:CreateAdminSession` et`wickr:ListNetworks`. Pour plus d'informations, consultez Exemples de politiques basées sur l'identité pour AWS Wickr et AWS politique gérée : AWSWickr FullAccess.

Validation de la conformité

Pour une liste des AWS services concernés par des programmes de conformité spécifiques, voir AWS Services concernés par programme de conformitéAWS . 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 lorsque vous utilisez Wickr 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 :

- Guides de démarrage rapide sur la sécurité et la conformité Guides sur la sécurité et la conformité — Ces guides de déploiement abordent les considérations architecturales et fournissent les étapes à suivre pour déployer des environnements de base axés sur la sécurité et la conformité sur. AWS
- 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.
- Évaluation des ressources à l'aide des règles énoncées dans le guide du AWS Config développeur : AWS Configévalue dans quelle mesure les configurations de vos ressources sont conformes aux pratiques internes, aux directives du secteur et aux réglementations.
- AWS Security Hub CSPM— Ce AWS service fournit une vue complète de l'état de votre sécurité interne, AWS ce qui vous permet de vérifier votre conformité aux normes et aux meilleures pratiques du secteur de la sécurité.

Résilience dans AWS Wickr

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, Wickr propose plusieurs fonctionnalités pour répondre à vos besoins en matière de résilience et de sauvegarde des données. Pour de plus amples informations, veuillez consulter Conservation des données pour AWS Wickr.

AWS PrivateLink pour AWS Wickr

Avec AWS PrivateLink AWS Wickr, vous pouvez établir une connexion privée entre votre Virtual Private Cloud (VPC) et un sous-ensemble de points de terminaison dans AWS Wickr en utilisant les points de terminaison VPC d'interface. Les points de terminaison VPC d'interface sont alimentés par AWS PrivateLink une AWS technologie que vous pouvez utiliser pour accéder aux services exécutés à l'aide AWS d'adresses IP privées.

Pour les clients mobiles ou autres appareils sur site, utilisez un VPN pour connecter votre appareil au VPC afin d'obtenir une connectivité privée de bout en bout. Pour plus d'informations, consultez la documentation AWS Virtual Private Network.

Pour plus d'informations sur le AWS PrivateLink AWS VPC, consultez Qu'est-ce que c'est ? AWS PrivateLink dans le AWS PrivateLink guide et qu'est-ce que le AWS VPC ? dans le guide de l'utilisateur d'Amazon Virtual Private Cloud.

Services AWS Wickr pris en charge

Les services AWS Wickr suivants sont pris en charge AWS PrivateLink :

Service	Format du terminal
Administrateur AWS Wickr	`com.amazonaws.` *`your-region`* `.wickr-admin`
Messagerie AWS Wickr	`com.amazonaws.` *`your-region`* `.wickr-messaging`
Appels AWS Wickr	`com.amazonaws.` *`your-region`* `.wickr-calling`

Tous les points de terminaison VPC Wickr nécessitent actuellement l'activation des noms DNS privés. Pour plus d'informations, voir Activer les noms DNS privés.

Les points de terminaison Wickr VPC prennent en charge le protocole FIPS dans les régions où les points de terminaison Wickr publics prennent en charge le protocole FIPS. Pour plus d'informations, consultez la norme fédérale de traitement de l'information.

Non pris en charge actuellement

- Politiques de point de terminaison VPC pour les points de terminaison de messagerie et d'appel
- Les points de terminaison de messagerie et d'appel ne sont pas disponibles dans`us-east-1`.

Rubriques

Conditions préalables

Avant de créer des points de terminaison VPC, assurez-vous de remplir les conditions préalables suivantes :

1. Configuration VPC : un VPC correctement configuré avec des sous-réseaux dans plusieurs zones de disponibilité
2. Groupes de sécurité : groupes de sécurité appropriés autorisant le trafic HTTPS (port 443)
3. Résolution DNS : noms d'hôte DNS et résolutions DNS activés dans le VPC
4. Autorisations IAM : autorisations nécessaires pour créer et gérer les points de terminaison VPC

Créer des points de terminaison d'un VPC

Vous pouvez créer un point de terminaison VPC pour AWS Wickr Admin, Messaging, and Calling.

Suivez la procédure suivante pour créer un point de terminaison VPC à l'aide AWS de la console.

Étape 1 : Accédez à la console VPC

1. Connectez-vous à la console Amazon VPC.
2. Dans le panneau de navigation de gauche, sélectionnez Points de terminaison.
3. Choisissez Créer un point de terminaison.

Étape 2 : Configuration des paramètres du point de terminaison

1. Sous Catégorie de service, sélectionnez AWS les services.

2. Sous Nom du service, recherchez `wickr` et sélectionnez le service approprié :

   - Pour l'administrateur : `com.amazonaws.your-region.wickr-admin`
   - Pour la messagerie : `com.amazonaws.your-region.wickr-messaging`
   - Pour appeler : `com.amazonaws.your-region.wickr-calling`

Étape 3 : Configuration du réseau

1. Sous VPC, sélectionnez votre VPC cible.
2. Sous Sous-réseaux, choisissez des sous-réseaux dans plusieurs zones de disponibilité pour une haute disponibilité.
3. Sous Activer le nom DNS privé, cochez la case. Cela permet de prendre en charge les noms DNS privés.
4. Sous Groupes de sécurité, sélectionnez ou créez des groupes de sécurité que vous souhaitez associer aux interfaces réseau des terminaux.

Étape 4 : créer un point de terminaison

1. Examinez votre configuration.
2. En option, vous pouvez ajouter ou supprimer des balises. Les balises sont des paires nom-valeur que vous utilisez pour associer à votre point de terminaison.
3. Choisissez Créer un point de terminaison.

Procédez comme suit pour créer un point de terminaison VPC à l'aide de. AWS CLI

1. Vérifiez la disponibilité du service dans votre région :

   Vérifiez la disponibilité de Wickr Admin

   ```
   aws ec2 describe-vpc-endpoint-services --service-names com.amazonaws.your-region.wickr-admin
   ```

   Vérifiez la disponibilité de Wickr Messaging

   ```
   aws ec2 describe-vpc-endpoint-services --service-names com.amazonaws.your-region.wickr-messaging
   ```

Vérifiez la disponibilité de Wickr Calling

```
aws ec2 describe-vpc-endpoint-services --service-names com.amazonaws.your-
region.wickr-calling
```

2. Créez des points de terminaison VPC.

   Point de terminaison Wickr Admin :

```
aws ec2 create-vpc-endpoint \
  --vpc-endpoint-type Interface \
  --service-name com.amazonaws.your-region.wickr-admin \
  --subnet-ids subnet-12345678 subnet-87654321 subnet-11223344 \
  --vpc-id vpc-12345678 \
  --security-group-ids sg-12345678 \
  --private-dns-enabled \
```

   Point de terminaison de messagerie Wickr

```
aws ec2 create-vpc-endpoint \
  --vpc-endpoint-type Interface \
  --service-name com.amazonaws.your-region.wickr-messaging \
  --subnet-ids subnet-12345678 subnet-87654321 subnet-11223344 \
  --vpc-id vpc-12345678 \
  --security-group-ids sg-12345678 \
  --private-dns-enabled \
```

   Point de terminaison d'appel Wickr

```
aws ec2 create-vpc-endpoint \
  --vpc-endpoint-type Interface \
  --service-name com.amazonaws.your-region.wickr-calling \
  --subnet-ids subnet-12345678 subnet-87654321 subnet-11223344 \
  --vpc-id vpc-12345678 \
  --security-group-ids sg-12345678 \
  --private-dns-enabled \
```

Limitations

Les fonctionnalités suivantes ne sont pas prises en charge via Internet AWS PrivateLink et nécessitent une connexion Internet :

- Accès libre en Wickr (WOA)
- Mises à jour des applications client
  - Applications mobiles (iOS/Android)
    - Source : App Store/Google Play Store
    - Exigence : accès à Internet requis
  - Applications de bureau
    - Windows/Mac : utilise des points de terminaison S3 globaux (non compatible) AWS PrivateLink
    - Linux : utilise Snap Store (nécessite un accès Internet)
- Débogage et télémétrie
  - Rapports de crash
  - Métriques de débogage
  - Liens d'analyse côté client
- Notifications push mobile

  Ces services nécessitent une connexion Internet et ne peuvent pas utiliser AWS PrivateLink :
  - Notifications Apple Push
    - Exigence : accès direct à Internet
    - Ports : 443, 2195, 2196, 5223
    - Référence : documentation de support Apple
  - Notifications Google/Android
    - Exigence : accès à Firebase Cloud Messaging
    - Référence : Documentation Firebase
- La console AWS Wickr n'est actuellement pas prise en charge pour l'accès privé. Pour plus d'informations, consultez Supportées Régions AWS, consoles de service et fonctionnalités de l'accès privé.

Versions client minimales requises pour AWS PrivateLink

Les versions clientes suivantes ont été validées avec AWS PrivateLink :

- iOS 6.64 (le cas échéant)
- Android 6.60 (le cas échéant)
- Clients de bureau 6.60
- Bottes 6.60

Fonctionnalités nécessitant une configuration supplémentaire

Bottes en osier

- Exigence : infrastructure gérée par le client
- Action : configurer les chemins réseau pour les dépendances des robots
- Considération : Assurez-vous que les robots peuvent accéder AWS aux services requis via les points de terminaison VPC

Téléchargements de fichiers

- Connectivité S3 : requise pour les opérations sur les fichiers (sauf dans la région de Francfort)
- Solution : créer un point de terminaison de passerelle VPC S3
- Référence : AWS PrivateLink pour Amazon S3

Sécurité de l'infrastructure dans AWS Wickr

En tant que service géré, AWS Wickr est protégé par les procédures de sécurité du réseau AWS mondial décrites dans le livre blanc Amazon Web Services : présentation des processus de sécurité.

Analyse de configuration et de vulnérabilité dans AWS Wickr

La configuration et les contrôles informatiques sont une responsabilité partagée entre vous AWS et vous, notre client. Pour plus d'informations, consultez le modèle de responsabilité AWS partagée.

Il est de votre responsabilité de configurer Wickr conformément aux spécifications et aux directives, de demander périodiquement à vos utilisateurs de télécharger la dernière version du client Wickr, de

vous assurer que vous utilisez la dernière version du bot de conservation des données Wickr et de surveiller l'utilisation de Wickr par vos utilisateurs.

Bonnes pratiques de sécurité pour AWS Wickr

Wickr fournit un certain nombre de fonctionnalités de sécurité à prendre en compte lorsque vous développez et mettez en œuvre 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.

Pour prévenir les événements de sécurité potentiels associés à votre utilisation de Wickr, suivez les meilleures pratiques suivantes :

- Implémentez l'accès avec le moindre privilège et créez des rôles spécifiques à utiliser pour les actions Wickr. Utilisez des modèles IAM pour créer un rôle. Pour de plus amples informations, veuillez consulter AWS politiques gérées pour AWS Wickr.
- Accédez au AWS Management Console for Wickr en vous authentifiant auprès du AWS Management Console premier. Ne partagez pas vos informations d'identification personnelles sur la console. Tous les utilisateurs d'Internet peuvent accéder à la console, mais ils ne peuvent pas se connecter ou démarrer une session s'ils n'ont pas d'informations d'identification valides pour la console.

Surveillance d'AWS Wickr

La surveillance joue un rôle important dans le maintien de la fiabilité, de la disponibilité et des performances d'AWS Wickr et de vos autres AWS solutions. AWS fournit les outils de surveillance suivants pour surveiller Wickr, signaler un problème et prendre des mesures automatiques le cas échéant :

- 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. Pour plus d'informations sur la journalisation des appels d'API Wickr à l'aide CloudTrail de. Journalisation des appels d'API AWS Wickr à l'aide de AWS CloudTrail

Journalisation des appels d'API AWS Wickr à l'aide de AWS CloudTrail

AWS Wickr est intégré à AWS CloudTrail un service qui fournit un enregistrement des actions entreprises par un utilisateur, un rôle ou un AWS service dans Wickr. CloudTrail capture tous les appels d'API pour Wickr sous forme d'événements. Les appels capturés incluent des appels provenant de AWS Management Console for Wickr et des appels de code vers les opérations de l'API Wickr. Si vous créez un suivi, vous pouvez activer la diffusion continue d' CloudTrail événements vers un compartiment Amazon S3, y compris des événements pour Wickr. Si vous ne configurez pas de suivi, vous pouvez toujours consulter les événements les plus récents dans la CloudTrail console dans Historique des événements. À l'aide des informations collectées par CloudTrail, vous pouvez déterminer la demande qui a été faite à Wickr, l'adresse IP à partir de laquelle la demande a été faite, qui a fait la demande, quand elle a été faite et des détails supplémentaires. Pour en savoir plus CloudTrail, consultez le guide de AWS CloudTrail l'utilisateur.

Informations sur Wickr dans CloudTrail

CloudTrail est activé sur votre compte Compte AWS lorsque vous créez le compte. Lorsqu'une activité se produit dans Wickr, cette activité est enregistrée dans un CloudTrail événement avec d'autres événements de AWS service dans l'historique des événements. Vous pouvez afficher,

rechercher et télécharger les événements récents dans votre Compte AWS. Pour plus d'informations, consultez la section Affichage des événements à l'aide de l'historique des CloudTrail événements.

Pour un enregistrement continu des événements de votre région Compte AWS, y compris des événements pour Wickr, créez un parcours. Un suivi permet CloudTrail de fournir des fichiers journaux à un compartiment Amazon S3. Par défaut, lorsque vous créez un journal d'activité dans la console, il s'applique à toutes les régions Régions AWS. Le journal enregistre les événements de toutes les régions de la AWS partition et transmet les fichiers journaux au compartiment Amazon S3 que vous spécifiez. En outre, vous pouvez configurer d'autres AWS services pour analyser plus en détail les données d'événements collectées dans les CloudTrail journaux et agir en conséquence. Pour plus d'informations, consultez les ressources suivantes :

- Présentation de la création d'un journal de suivi
- CloudTrail services et intégrations pris en charge
- Configuration des notifications Amazon SNS pour CloudTrail
- Réception de fichiers CloudTrail journaux de plusieurs régions et réception de fichiers CloudTrail journaux de plusieurs comptes

Toutes les actions de Wickr sont enregistrées par CloudTrail. Par exemple, les appels au `CreateAdminSession` et les `ListNetworks` actions génèrent des entrées dans les fichiers CloudTrail journaux.

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 les éléments suivants :

- Si la demande a été faite avec les informations d'identification de l'utilisateur root ou Gestion des identités et des accès AWS (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 demande a été faite par un autre AWS service.

Pour de plus amples informations, veuillez consulter l'élément userIdentity CloudTrail .

Comprendre les entrées du fichier journal Wickr

Un suivi est une configuration qui permet de transmettre des événements sous forme de fichiers journaux à un compartiment Amazon S3 que vous spécifiez. CloudTrail les fichiers journaux

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

L'exemple suivant montre une entrée de CloudTrail journal illustrant l'`CreateAdminSession`action.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "<principal-id>",
        "arn": "<arn>",
        "accountId": "<account-id>",
        "accessKeyId": "<access-key-id>",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "<principal-id>",
                "arn": "<arn>",
                "accountId": "<account-id>",
                "userName": "<user-name>"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-03-10T07:53:17Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-03-10T08:19:24Z",
    "eventSource": "wickr.amazonaws.com",
    "eventName": "CreateAdminSession",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "<ip-address>",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
 like Gecko) Chrome/110.0.0.0 Safari/537.36",
    "requestParameters": {
        "networkId": 56019692
    },
    "responseElements": {
        "sessionCookie": "***",
```

```
        "sessionNonce": "***"
    },
    "requestID": "39ed0e6f-36e9-460d-8a6e-f24be0ec11c5",
    "eventID": "98ccb633-0e6c-4325-8996-35c3043022ac",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "<account-id>",
    "eventCategory": "Management"
}
```

L'exemple suivant montre une entrée de CloudTrail journal illustrant l'`CreateNetwork`action.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "<principal-id>",
        "arn": "<arn>",
        "accountId": "<account-id>",
        "accessKeyId": "<access-key-id>",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "<principal-id>",
                "arn": "<arn>",
                "accountId": "<account-id>",
                "userName": "<user-name>"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-03-10T07:53:17Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-03-10T07:54:09Z",
    "eventSource": "wickr.amazonaws.com",
    "eventName": "CreateNetwork",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "<ip-address>",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
 like Gecko) Chrome/110.0.0.0 Safari/537.36",
```

```
    "requestParameters": {
        "networkName": "BOT_Network",
        "accessLevel": "3000"
    },
    "responseElements": null,
    "requestID": "b83c0b6e-73ae-45b6-8c85-9910f64d33a1",
    "eventID": "551277bb-87e0-4e66-b2a0-3cc1eff303f3",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "<account-id>",
    "eventCategory": "Management"
}
```

L'exemple suivant montre une entrée de CloudTrail journal illustrant l'`ListNetworks`action.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "<principal-id>",
        "arn": "<arn>",
        "accountId": "<account-id>",
        "accessKeyId": "<access-key-id>",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "<principal-id>",
                "arn": "<arn>",
                "accountId": "<account-id>",
                "userName": "<user-name>"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-03-10T12:19:39Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-03-10T12:29:32Z",
    "eventSource": "wickr.amazonaws.com",
    "eventName": "ListNetworks",
    "awsRegion": "us-east-1",
```

```
    "sourceIPAddress": "<ip-address>",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
 like Gecko) Chrome/110.0.0.0 Safari/537.36",
    "requestParameters": null,
    "responseElements": null,
    "requestID": "b9800ba8-541a-43d1-9c8e-efd94d5f2115",
    "eventID": "5fbc83d7-771b-457d-9329-f85163a6a428",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "<account-id>",
    "eventCategory": "Management"
}
```

L'exemple suivant montre une entrée de CloudTrail journal illustrant l'`UpdateNetworkdetails`action.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "<principal-id>",
        "arn": "<arn>",
        "accountId": "<account-id>",
        "accessKeyId": "<access-key-id>",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "<principal-id>",
                "arn": "<arn>",
                "accountId": "<account-id>",
                "userName": "<user-name>"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-03-08T22:42:15Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-03-08T22:42:58Z",
    "eventSource": "wickr.amazonaws.com",
    "eventName": "UpdateNetworkDetails",
```

```
    "awsRegion": "us-east-1",
    "sourceIPAddress": "<ip-address>",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/110.0.0.0 Safari/537.36",
    "requestParameters": {
        "networkName": "CloudTrailTest1",
        "networkId": <network-id>
    },
    "responseElements": null,
    "requestID": "abced980-23c7-4de1-b3e3-56aaf0e1fdbb",
    "eventID": "a4dc3391-bdce-487d-b9b0-6f76cedbb198",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "<account-id>",
    "eventCategory": "Management"
}
```

L'exemple suivant montre une entrée de CloudTrail journal illustrant l'`TagResource`action.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "<principal-id>",
        "arn": "<arn>",
        "accountId": "<account-id>",
        "accessKeyId": "<access-key-id>",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "<principal-id>",
                "arn": "<arn>",
                "accountId": "<account-id>",
                "userName": "<user-name>"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-03-08T22:42:15Z",
                "mfaAuthenticated": "false"
            }
        }
    },
```

```
    "eventTime": "2023-03-08T23:06:04Z",
    "eventSource": "wickr.amazonaws.com",
    "eventName": "TagResource",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "<ip-address>",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/110.0.0.0 Safari/537.36",
    "requestParameters": {
        "resource-arn": "<arn>",
        "tags": {
            "some-existing-key-3": "value 1"
        }
    },
    "responseElements": null,
    "requestID": "4ff210e1-f69c-4058-8ac3-633fed546983",
    "eventID": "26147035-8130-4841-b908-4537845fac6a",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "<account-id>",
    "eventCategory": "Management"
}
```

L'exemple suivant montre une entrée de CloudTrail journal illustrant l'`ListTagsForResource`action.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "<principal-id>",
        "arn": "<arn>",
        "accountId": "<account-id>",
        "accessKeyId": "<access-key-id>",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "<access-key-id>",
                "arn": "<arn>",
                "accountId": "<account-id>",
                "userName": "<user-name>"
            },
            "webIdFederationData": {},
            "attributes": {
```

```
                "creationDate": "2023-03-08T18:50:37Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-03-08T18:50:37Z",
    "eventSource": "wickr.amazonaws.com",
    "eventName": "ListTagsForResource",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "<ip-address>",
    "userAgent": "axios/0.27.2",
    "errorCode": "AccessDenied",
    "requestParameters": {
        "resource-arn": "<arn>"
    },
    "responseElements": {
        "message": "User: <arn> is not authorized to perform: wickr:ListTagsForResource
 on resource: <arn> with an explicit deny"
    },
    "requestID": "c7488490-a987-4ca2-a686-b29d06db89ed",
    "eventID": "5699d5de-3c69-4fe8-b353-8ae62f249187",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "<account-id>",
    "eventCategory": "Management"
}
```


Tableau de bord d'analyse dans AWS Wickr

Vous pouvez utiliser le tableau de bord d'analyse pour voir comment votre organisation utilise AWS Wickr. La procédure suivante explique comment accéder au tableau de bord d'analyse à l'aide de la console AWS Wickr.

Pour accéder au tableau de bord d'analyse

1. Ouvrez le AWS Management Console pour Wickr à l'adresse https://console.aws.amazon.com/wickr/.
2. Sur la page Réseaux, sélectionnez le nom du réseau pour accéder à ce réseau.
3. Dans le volet de navigation, sélectionnez Analytics (Analyse).

La page Analytics affiche les statistiques de votre réseau dans différents onglets.

Sur la page Analytics, vous trouverez un filtre de période dans le coin supérieur droit de chaque onglet. Ce filtre s'applique à l'ensemble de la page. En outre, dans le coin supérieur droit de chaque onglet, vous pouvez exporter les points de données pour la plage de temps sélectionnée en choisissant l'option Exporter disponible.

> **Note**
>
> L'heure sélectionnée est en UTC (temps universel coordonné).

Les onglets suivants sont disponibles :

- La vue d'ensemble s'affiche :
  - Enregistré : nombre total d'utilisateurs enregistrés, y compris les utilisateurs actifs et suspendus sur le réseau pendant la période sélectionnée. Il n'inclut pas les utilisateurs en attente ou invités.
  - En attente : nombre total d'utilisateurs en attente sur le réseau pendant la période sélectionnée.
  - Enregistrement des utilisateurs — Le graphique affiche le nombre total d'utilisateurs enregistrés dans la période sélectionnée.
  - Appareils : nombre d'appareils sur lesquels l'application a été active.
  - Versions clientes : nombre d'appareils actifs classés selon leur version client.

- Les membres affichent :
  - État : utilisateurs actifs sur le réseau pendant la période sélectionnée.
  - Utilisateurs actifs —
    - Le graphique affiche le nombre d'utilisateurs actifs au fil du temps et peut être agrégé par jour, par semaine ou par mois (dans la plage de temps sélectionnée ci-dessus).
    - Le nombre d'utilisateurs actifs peut être ventilé par plate-forme, version du client ou groupe de sécurité. Si un groupe de sécurité a été supprimé, le nombre total sera affiché sous la forme Supprimé#.

- Les messages s'affichent :

- Messages envoyés : nombre de messages uniques envoyés par tous les utilisateurs et robots du réseau au cours de la période sélectionnée.
- Appels : nombre d'appels uniques effectués par tous les utilisateurs du réseau.
- Fichiers : nombre de fichiers envoyés par les utilisateurs du réseau (y compris les mémos vocaux).
- Appareils : le graphique circulaire indique le nombre de périphériques actifs classés par système d'exploitation.
- Versions clientes : nombre d'appareils actifs classés selon leur version client.

Historique du document

Le tableau suivant décrit les versions de documentation de Wickr.

Modification	Description	Date
L'aperçu du fichier est désormais disponible	Les administrateurs de Wickr ont désormais la possibilité d'activer ou de désactiver le téléchargement de fichiers. Pour plus d'informations, consultez la section Aperçu du fichier pour AWS Wickr.	29 mai 2025
La console d'administration Wickr récemment repensée est désormais disponible	Wickr a amélioré la console d'administration Wickr pour une meilleure navigation et une meilleure accessibilité pour les administrateurs.	13 mars 2025
Wickr est désormais disponible en Asie-Pacifique (Malaisie) Région AWS	Wickr est désormais disponible en Asie-Pacifique (Malaisie). Région AWS Pour plus d'informations, consultez la section Disponibilité régionale.	20 novembre 2024
Supprimer le réseau est désormais disponible	Les administrateurs Wickr ont désormais la possibilité de supprimer un réseau AWS Wickr. Pour plus d'informations, consultez Supprimer le réseau dans AWS Wickr.	4 octobre 2024
La configuration d'AWS Wickr avec Microsoft Entra (Azure AD) SSO est désormais disponible	AWS Wickr peut être configuré pour utiliser Microsoft Entra (Azure AD) en tant que fournisseur d'identité. Pour	18 septembre 2024

	plus d'informations, consultez Configurer AWS Wickr avec l'authentification unique Microsoft Entra (Azure AD).	
Wickr est désormais disponible en Europe (Zurich) Région AWS	Wickr est désormais disponible en Europe (Zurich). Région AWS Pour plus d'informations, consultez la section Disponibilité régionale.	12 août 2024
La classification et la fédération transfrontalières sont désormais disponibles	La fonction de classification transfrontalière permet de modifier l'interface utilisateur dans les conversations des GovCloud utilisateurs. Pour plus d'informations, voir Classification GovCloud transfrontalière et fédération.	25 juin 2024
La fonction de lecture du reçu est désormais disponible	Les administrateurs de Wickr peuvent désormais activer ou désactiver la fonction de confirmation de lecture dans la console d'administration. Pour plus d'informations, consultez la section Lire les reçus.	23 avril 2024

Global Federation prend désormais en charge la fédération restreinte et les administrateurs peuvent consulter les analyses d'utilisation dans la console d'administration	La Fédération mondiale prend désormais en charge la fédération restreinte. Cela fonctionne pour les réseaux Wickr dans d'autres Régions AWS. Pour plus d'informations, consultez la section Groupes de sécurité. En outre, les administrateurs peuvent désormais consulter leurs analyses d'utilisation sur le tableau de bord Analytics de la console d'administration. Pour plus d'informations, consultez le tableau de bord Analytics.	28 mars 2024
Un essai gratuit de trois mois du plan Premium d'AWS Wickr est désormais disponible	Les administrateurs de Wickr peuvent désormais choisir un plan Premium d'essai gratuit de trois mois pour un maximum de 30 utilisateurs. Pendant l'essai gratuit, toutes les fonctionnalités des forfaits Standard et Premium sont disponibles, y compris les contrôles administratifs illimités et la conservation des données. La fonctionnalité d'utilisateur invité n'est pas disponible pendant l'essai gratuit Premium. Pour plus d'informations, consultez la section Gérer le plan.	9 février 2024

La fonctionnalité d'utilisateur invité est généralement disponible et d'autres contrôles d'administrateur ont été ajoutés.	Les administrateurs de Wickr peuvent désormais accéder à une série de nouvelles fonctionnalités, notamment la liste des utilisateurs invités, la possibilité de supprimer ou de suspendre des utilisateurs en bloc, et la possibilité d'empêcher les utilisateurs invités de communiquer sur votre réseau Wickr. Pour plus d'informations, consultez la section Utilisateurs invités.	8 novembre 2023
Wickr est désormais disponible en Europe (Francfort) Région AWS	Wickr est désormais disponible en Europe (Francfort). Région AWS Pour plus d'informations, consultez la section Disponibilité régionale.	26 octobre 2023
Les réseaux Wickr ont désormais la capacité de se fédérer entre Régions AWS	Les réseaux Wickr ont désormais la capacité de se fédérer entre eux. Régions AWS Pour plus d'informations, consultez la section Groupes de sécurité.	29 septembre 2023
Wickr est désormais disponible en Europe (Londres) Région AWS	Wickr est désormais disponible en Europe (Londres). Région AWS Pour plus d'informations, consultez la section Disponibilité régionale.	23 août 2023

Wickr est maintenant disponible au Canada (Centre) Région AWS	Wickr est maintenant disponible au Canada (centre). Région AWS Pour plus d'informations, consultez la section Disponibilité régionale.	3 juillet 2023
La fonctionnalité utilisateur invité est désormais disponible en avant-première	Les utilisateurs invités peuvent se connecter au client Wickr et collaborer avec les utilisateurs du réseau Wickr. Pour plus d'informations, consultez la section Utilisateurs invités (aperçu).	31 mai 2023
AWS Wickr est désormais intégré à AWS CloudTrail et est désormais disponible dans AWS GovCloud (ouest des États-Unis) en tant que WickrGov	AWS Wickr est désormais intégré à AWS CloudTrail. Pour plus d'informations, consultez la section Journalisation des appels d'API AWS Wickr à l'aide AWS CloudTrail de. De plus, Wickr est désormais disponible en AWS GovCloud (ouest des États-Unis) sous forme de. WickrGov Pour plus d'informations, consultez AWS WickrGov dans le Guide de l'utilisateur AWS GovCloud (US) .	30 mars 2023

Balisage et création de réseaux multiples	Le balisage est désormais pris en charge dans AWS Wickr. Pour plus d'informations, consultez la section Balises réseau. Plusieurs réseaux peuvent désormais être créés dans Wickr. Pour plus d'informations, consultez la section Création d'un réseau.	7 mars 2023
Première version	Publication initiale du guide d'administration de Wickr	28 novembre 2022

Notes de mise à jour

Pour vous aider à suivre les mises à jour et améliorations continues de Wickr, nous publions des avis de publication décrivant les modifications récentes.

août 2025

- Les modèles d'e-mail pour AWS Wickr AWS WickrGov ont été mis à jour afin d'améliorer l'expérience d'intégration des utilisateurs. L'adresse e-mail de l'expéditeur est passée de `donotreply@wickr.email` à`no-reply@amazonaws.com`.

Mai 2025

- L'aperçu du fichier est désormais disponible. Lorsque les téléchargements de fichiers sont désactivés par l'administrateur dans la console d'administration d'un groupe de sécurité, les utilisateurs peuvent uniquement consulter la liste des fichiers pris en charge dans les onglets Messagerie et Fichiers.

Mars 2025

- La console d'administration Wickr redessinée est désormais disponible.

Octobre 2024

- Wickr prend désormais en charge la suppression du réseau. Pour plus d'informations, consultez Supprimer le réseau dans AWS Wickr.

Septembre 2024

- Les administrateurs peuvent désormais configurer AWS Wickr avec l'authentification unique Microsoft Entra (Azure AD). Pour plus d'informations, consultez Configurer AWS Wickr avec l'authentification unique Microsoft Entra (Azure AD).

août 2024

- Améliorations
  - Wickr est désormais disponible en Europe (Zurich). Région AWS

Juin 2024

- La classification et la fédération transfrontalières sont désormais disponibles pour GovCloud les utilisateurs. Pour plus d'informations, voir Classification GovCloud transfrontalière et fédération.

Avril 2024

- Wickr prend désormais en charge les reçus de lecture. Pour plus d'informations, voir Lire les reçus.

Mars 2024

- La fédération mondiale prend désormais en charge la fédération restreinte, où la fédération mondiale ne peut être activée que pour certains réseaux ajoutés dans le cadre d'une fédération restreinte. Cela fonctionne pour les réseaux Wickr dans d'autres Régions AWS. Pour plus d'informations, consultez la section Groupes de sécurité.
- Les administrateurs peuvent désormais consulter leurs analyses d'utilisation sur le tableau de bord Analytics de la console d'administration. Pour plus d'informations, consultez le tableau de bord Analytics.

Février 2024

- AWS Wickr propose désormais un essai gratuit de trois mois de son plan Premium pour un maximum de 30 utilisateurs. Les modifications et les limites incluent :
  - Toutes les fonctionnalités des forfaits Standard et Premium, telles que les contrôles administratifs illimités et la conservation des données, sont désormais disponibles dans le cadre de l'essai gratuit Premium. La fonctionnalité d'utilisateur invité n'est pas disponible pendant l'essai gratuit Premium.

- L'essai gratuit précédent n'est plus disponible. Vous pouvez passer de votre essai gratuit ou de votre forfait Standard à un essai gratuit Premium si vous n'avez pas encore utilisé l'essai gratuit Premium. Pour plus d'informations, consultez la section Gérer le plan.

Novembre 2023

- La fonctionnalité réservée aux utilisateurs invités est désormais disponible pour tous. Les modifications et les ajouts incluent :
  - Possibilité de signaler les abus commis par d'autres utilisateurs de Wickr.
  - Les administrateurs peuvent consulter la liste des utilisateurs invités avec lesquels un réseau a interagi, ainsi que le nombre d'utilisateurs mensuels.
  - Les administrateurs peuvent empêcher les utilisateurs invités de communiquer avec leur réseau.
  - Tarifs supplémentaires pour les utilisateurs invités.

- Améliorations du contrôle administratif
  - Possibilité de regrouper les delete/suspend utilisateurs.
  - Paramètre SSO supplémentaire pour configurer une période de grâce pour l'actualisation des jetons.

Octobre 2023

- Améliorations
  - Wickr est désormais disponible en Europe (Francfort). Région AWS

Septembre 2023

- Améliorations
  - Les réseaux Wickr ont désormais la capacité de se fédérer entre eux. Régions AWS Pour plus d'informations, consultez la section Groupes de sécurité.

août 2023

- Améliorations
  - Wickr est désormais disponible en Europe (Londres). Région AWS

Juillet 2023

- Améliorations
  - Wickr est maintenant disponible au Canada (centre). Région AWS

Mai 2023

- Améliorations
  - Support supplémentaire pour les utilisateurs invités. Pour de plus amples informations, veuillez consulter Utilisateurs invités du réseau AWS Wickr.

Mars 2023

- Wickr est désormais intégré à AWS CloudTrail. Pour de plus amples informations, veuillez consulter Journalisation des appels d'API AWS Wickr à l'aide de AWS CloudTrail.
- Wickr est désormais disponible en AWS GovCloud (ouest des États-Unis) sous forme de. WickrGov Pour plus d'informations, consultez AWS WickrGov dans le Guide de l'utilisateur AWS GovCloud (US) .
- Wickr prend désormais en charge le balisage. Pour de plus amples informations, veuillez consulter Balises réseau pour AWS Wickr. Plusieurs réseaux peuvent désormais être créés dans Wickr. Pour de plus amples informations, veuillez consulter Étape 1 : créer un réseau.

Février 2023

- Wickr prend désormais en charge le kit d'assaut tactique Android (ATAK). Pour de plus amples informations, veuillez consulter Activez ATAK dans le tableau de bord du réseau Wickr.

janvier 2023

- L'authentification unique (SSO) peut désormais être configurée sur tous les forfaits, y compris l'essai gratuit et le forfait Standard.

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.