Guide d'administration de la console

AWS Re:Publier en mode privé

AWS Re:Publier en mode privé: Guide d'administration de la console

Table of Contents

Qu'est-ce qu'AWS Re:Post Private ?

AWS Re:Post Private est une version privée d'AWS Re:Post destinée aux entreprises disposant de plans Enterprise Support ou Enterprise On-Ramp Support. Il donne accès à des connaissances et à des experts pour accélérer l'adoption du cloud et augmenter la productivité des développeurs. Avec Re:Post privé spécifique à votre organisation, vous pouvez créer une communauté de développeurs spécifique à votre organisation qui améliore l'efficacité à grande échelle et donne accès à de précieuses ressources de connaissances. En outre, Re:post Private centralise le contenu AWS technique fiable et propose des forums de discussion privés pour améliorer la façon dont vos équipes collaborent en interne et avec AWS afin de supprimer les obstacles techniques, d'accélérer l'innovation et d'évoluer plus efficacement dans le cloud.

Pour plus d'informations, consultez AWS re:Post Private.

Accédez à Re:Post Private

Les administrateurs utilisent la console AWS Re:POST Private pour créer le Re:POST privé spécifique à leur organisation. Lorsque les administrateurs créent un Re:POST privé, ils peuvent le nommer Re:POST privé et définir un sous-domaine sous. `*.private.repost.aws` Les administrateurs du Re:POST privé d'une organisation peuvent configurer l'accès des utilisateurs en utilisant AWS IAM Identity Center et en spécifiant l'une des sources d'identité suivantes pour l'authentification : annuaire Identity Center, Active Directory ou fournisseur d'identité externe. Après avoir configuré les utilisateurs, les administrateurs de console peuvent attribuer un rôle d'administrateur Re:Post Private à un ou plusieurs utilisateurs. Les administrateurs de re:Post Private peuvent personnaliser leur application privée Re:POST conformément à l'image de marque et aux besoins de connaissances de l'organisation. Les membres de l'équipe chargée du AWS compte, tels que les responsables techniques des comptes, qui connaissent bien l'architecture et les charges de travail de l'organisation sont automatiquement ajoutés au fichier privé Re:POST de l'organisation à des fins de collaboration.

Les administrateurs de l'application Re:Post Private peuvent personnaliser l'image de marque, ajouter des balises pour classer le contenu et sélectionner des sujets d'intérêt pour leurs développeurs afin de renseigner automatiquement le contenu technique et de formation. Ils peuvent également inviter les utilisateurs à rejoindre leur Re:POST privé pour une collaboration accrue. Pour plus d'informations, consultez le guide d'administration privée d'AWS re:Post.

Les utilisateurs non administrateurs utilisent l'application Re:Post Private pour se connecter à l'aide des informations d'identification configurées par leur administrateur. Une fois connectés à un Re:post privé, les utilisateurs peuvent parcourir ou rechercher du contenu existant, y compris des formations personnalisées et du contenu technique adapté à leurs sujets d'intérêt. Les utilisateurs peuvent également rechercher du contenu technique AWS public directement à partir de leur Re:post privé et créer des fils de discussion privés pour les discussions internes sur le contenu AWS public. Les utilisateurs peuvent résoudre des problèmes AWS techniques de manière collaborative et obtenir des conseils techniques de la part d'autres utilisateurs du service privé Re:post en posant une question, en fournissant une réponse ou en publiant un article. Les utilisateurs peuvent également convertir un fil de discussion en AWS Support dossier. Les utilisateurs peuvent choisir d'ajouter les réponses depuis AWS Support au Re:post privé. Pour plus d'informations, consultez le guide de l'utilisateur privé d'AWS re:Post.

Tarification

Seuls les clients disposant de plans Enterprise Support (ES) et Enterprise On-Ramp (EOP) Support peuvent s'abonner au service Re:post Private. Vous pouvez choisir entre les deux niveaux de tarification disponibles : le niveau gratuit et le niveau standard. Le niveau gratuit vous permet d'explorer et de tester pleinement les fonctionnalités du niveau Standard pendant six mois avant de passer facilement au niveau payant. Si vous utilisez le niveau Standard, vous pouvez payer un abonnement mensuel par utilisateur pour utiliser Re:Post Private. Pour plus d’informations, consultez Tarification d’.

Comment démarrer

Pour commencer à utiliser Re:Post Private, consultez. Prérequis

Prérequis

Vous devez remplir les conditions préalables suivantes avant de pouvoir créer un nouveau re:POST privé ou gérer un re:POST privé existant dans AWS re:Post Private :

- Vous devez souscrire à un plan de support Enterprise ou Enterprise On-Ramp.
- Vous devez l'activer AWS IAM Identity Center dans la même région que celle où vous souhaitez configurer votre Re:post privé.
- Vous devez créer un AWS Identity and Access Management rôle doté des autorisations requises pour créer, gérer et résoudre les AWS Support dossiers à votre place. Le service Re:Post Private utilise ce rôle pour effectuer des appels d'API à. AWS Support Pour plus d'informations, consultez Gestion de l'accès à AWS Support la création et à la gestion des dossiers dans Re:Post Private.

Intégrez Re:POST Private via IAM Identity Center

Re:Post Private s'intègre AWS IAM Identity Center pour fournir une fédération d'identité à votre personnel. Grâce à IAM Identity Center, les utilisateurs sont redirigés vers le répertoire de leur entreprise existant pour se connecter avec leurs informations d'identification existantes. Ensuite, ils sont facilement connectés à leur Re:post privé. Cela garantit que les paramètres de sécurité tels que les politiques de mot de passe et l'authentification à deux facteurs sont appliqués. L'utilisation d'IAM Identity Center n'a aucune incidence sur votre configuration IAM existante.

Si vous n'avez pas d'annuaire d'utilisateurs existant ou si vous préférez ne pas vous fédérer, IAM Identity Center propose un annuaire d'utilisateurs intégré que vous pouvez utiliser pour créer des utilisateurs et des groupes pour Re:Post Private. Re:Post Private ne prend pas en charge l'utilisation d'utilisateurs et de rôles IAM pour attribuer des autorisations au sein d'un Re:POST privé. Les autorisations utilisateur au sein d'un Re:Post privé sont configurées par un administrateur sur son application privée Re:Post.

Pour plus d'informations sur IAM Identity Center, consultez Qu'est-ce qu'AWS IAM Identity Center (successeur d'AWS Single Sign-On). Pour plus d'informations sur la prise en main d'IAM Identity Center, consultez Getting started. Pour utiliser IAM Identity Center, vous devez également avoir AWS Organizations activé le compte.

> **Important**
>
> RE:Post Private ne prend en charge que les instances organisationnelles d'IAM Identity Center.

Sécurité dans Re:Post Private

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

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

- Sécurité du cloud : AWS est chargée de protéger l'infrastructure qui exécute les AWS services dans le AWS Cloud. AWS vous fournit également des services que vous pouvez utiliser en toute sécurité. Des auditeurs tiers testent et vérifient régulièrement l'efficacité de notre sécurité dans le cadre des programmes de AWS conformité Programmes de de conformité. Pour en savoir plus sur les programmes de conformité qui s'appliquent à AWS re:Post Private, 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 la sensibilité de vos données, les exigences de votre entreprise, et la législation et la réglementation applicables.

Cette documentation vous aide à comprendre comment appliquer le modèle de responsabilité partagée lors de l'utilisation de RE:Post Private. Les rubriques suivantes expliquent comment configurer re:Post Private pour répondre à vos objectifs de sécurité et de conformité. Vous apprendrez également à utiliser d'autres AWS services qui vous aident à surveiller et à sécuriser vos ressources Re:post Private.

Rubriques

Protection des données dans AWS Re:Post Private

Le modèle de responsabilité AWS partagée s'applique à la protection des données dans AWS Re:Post Private. 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 AWS services que vous utilisez. Pour plus d'informations sur la confidentialité des données, consultez Questions fréquentes (FAQ) sur la confidentialité des données. Pour en savoir plus sur la protection des données en Europe, consultez le billet de blog Modèle de responsabilité partagée AWS et RGPD (Règlement général sur la protection des données) sur le Blog de sécuritéAWS .

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

- Utilisez l'authentification multifactorielle (MFA) avec chaque compte.
- Utilisez le protocole SSL/TLS pour communiquer avec les ressources. AWS Nous exigeons TLS 1.2 et recommandons TLS 1.3.
- Configurez l'API et la journalisation de l'activité des utilisateurs avec AWS CloudTrail.
- Utilisez des solutions de AWS chiffrement, ainsi que tous les contrôles de sécurité par défaut qu'ils contiennent AWS services.
- 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 140-2 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 (Federal Information Processing Standard) disponibles, consultez Federal Information Processing Standard (FIPS) 140-2 (Normes de traitement de l'information fédérale).

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 Name (Nom). Cela inclut lorsque vous travaillez avec Re:Post Private ou autre à AWS services l'aide de la console, de l'API ou AWS des AWS CLI SDK. 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.

Protection des données à l'aide du chiffrement

Chiffrement au repos

RE:Post Private utilise des compartiments Amazon Simple Storage Service, des bases de données Amazon DynamoDB, des bases de données Amazon Neptune OpenSearch et des domaines Amazon Service qui sont chiffrés au repos à l'aide de clés gérées par Amazon ou de clés gérées par le client.

Chiffrement en transit

RE:Post Private utilise le protocole HTTPS pour communiquer avec votre application cliente. Il utilise le protocole HTTPS et AWS des signatures pour communiquer avec d'autres services au nom de votre application.

Gestion des clés

RE:Post Private est intégré aux clés AWS Key Management Service et les prend en charge AWS KMS . Vous pouvez personnaliser les paramètres de chiffrement des données pour votre Re:Post privé lorsque vous le créez. Pour ce faire, vous pouvez choisir une AWS KMS clé existante ou en créer une nouvelle AWS KMS.

Comment Re:post Private fonctionne avec IAM

Avant d'utiliser IAM pour gérer l'accès à AWS Re:Post Private, vous devez comprendre quelles fonctionnalités IAM peuvent être utilisées avec Re:Post Private. Pour obtenir une vue d'ensemble du fonctionnement de Re:Post Private et des autres AWS services avec IAM, consultez la section AWS Services compatibles avec IAM dans le guide de l'utilisateur d'IAM.

Re:post Politiques basées sur l'identité privée

Avec les politiques basées sur l'identité IAM, vous pouvez spécifier des actions autorisées ou refusées. re:Post Private prend en charge des actions spécifiques. Pour en savoir plus sur les

éléments que vous utilisez dans une politique JSON, veuillez consulter Références des éléments de politique JSON IAM dans le Guide de l'utilisateur IAM.

Actions

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

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

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

Les actions politiques dans Re:post Private utilisent le préfixe suivant avant l'action :. `repostspace:` Par exemple, pour autoriser quelqu'un à exécuter l'opération d'`CreateSpace`API Re:Post Private, vous devez inclure l'`repostspace:CreateSpace`action dans sa politique. Les déclarations de politique doivent inclure un `NotAction` élément `Action` ou. Re:Post Private définit son propre ensemble d'actions décrivant les tâches que vous pouvez effectuer avec ce service.

Pour spécifier plusieurs actions dans une seule déclaration, séparez-les par des virgules comme suit :

```
"Action": [
      "repostspace:CreateSpace",
      "repostspace:DeleteSpace"
```

Vous pouvez aussi spécifier plusieurs actions à l'aide de caractères génériques (*). Par exemple, pour spécifier toutes les actions qui commencent par le mot `Describe`, incluez l'action suivante :

```
"Action": "repostspace:Describe*"
```

Pour consulter la liste des actions Re:Post Private, voir Actions définies par Re:Post Private dans le guide de l'utilisateur IAM.

Ressources

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

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

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

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

Clés de condition

RE:Post Private ne fournit aucune clé de condition spécifique au service, mais il prend en charge l'utilisation de clés de condition globales. 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.

Exemples

Pour consulter des exemples de politiques basées sur l'identité Re:Post Private, consultez. Exemples de politiques basées sur l'identité privée AWS Re:POST

Politiques basées sur les ressources privées Re:POST

Les politiques basées sur les ressources sont des documents de politique JSON que vous attachez à une ressource. Des politiques basées sur les ressources sont, par exemple, les politiques de confiance de rôle IAM et des politiques de compartiment. 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 AWS des services. 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.

re:Post Private ne prend pas en charge les politiques basées sur les ressources.

Autorisation basée sur les balises

Re:post Private permet de baliser les ressources ou de contrôler l'accès en fonction des balises. Pour plus d'informations, consultez la section Contrôle de l'accès aux ressources AWS à l'aide de balises.

Re : publier des rôles IAM privés

Un rôle IAM est une entité de votre AWS compte qui dispose d'autorisations spécifiques.

Utilisation d'informations d'identification temporaires avec Re:Post Private

Nous vous recommandons vivement d'utiliser des informations d'identification temporaires pour vous connecter à la fédération, assumer un rôle IAM ou assumer un rôle multicompte. Vous obtenez des informations d'identification de sécurité temporaires en appelant des opérations d' AWS STS API telles que AssumeRoleou GetFederationToken.

RE:Post Private prend en charge l'utilisation d'informations d'identification temporaires.

Rôles liés à un service

Les rôles liés aux AWS services permettent aux services d'accéder aux ressources d'autres services pour effectuer une action à votre place. Les rôles liés à un service s’affichent dans votre compte IAM et sont la propriété du service. Un administrateur IAM peut consulter, mais ne peut pas modifier, les autorisations concernant les rôles liés à un service.

Fonctions du service

Cette fonctionnalité permet à un service d'assumer un rôle de service à votre place. Ce rôle permet au service d'accéder aux ressources d'autres services pour effectuer une action à votre place. Pour plus d'informations, consultez Création d'un rôle pour déléguer des autorisations à un service AWS. Les rôles de service s’affichent dans votre compte IAM et sont la propriété du compte. Cela signifie qu’un administrateur IAM peut modifier les autorisations associées à ce rôle. Toutefois, une telle action peut perturber le bon fonctionnement du service.

Utilisation de rôles liés à un service pour Re:Post Private

AWS Re:POST Private utilise des rôles liés à un AWS Identity and Access Management service (IAM). Un rôle lié à un service est un type unique de rôle IAM directement lié à Re:Post Private. Les rôles liés à un service sont prédéfinis par Re:Post Private et incluent toutes les autorisations dont le service a besoin pour appeler d'autres AWS services en votre nom.

Un rôle lié à un service facilite la configuration de Re:Post Private, car vous n'avez pas à ajouter manuellement les autorisations nécessaires. Re:Post Private définit les autorisations de ses rôles liés au service et, sauf indication contraire, seul Re:Post Private peut assumer ses rôles. Les autorisations définies comprennent la politique d'approbation et la politique d'autorisation. De plus, cette politique d'autorisation ne peut pas être attachée à une autre entité IAM.

Pour plus d'informations sur les autres services qui prennent en charge les rôles liés à un service, consultez Services AWS qui fonctionnent avec IAM et recherchez les services présentant la mention Yes (Oui) dans la colonne Service-linked roles (Rôles liés à un service). Sélectionnez un Oui ayant un lien pour consulter la documentation du rôle lié à un service, pour ce service.

Autorisations de rôle liées au service pour Re:Post Private

re:Post Private utilise le rôle lié au service nommé AWSServiceRoleForrePostPrivate. re:Post Private utilise ce rôle lié au service pour publier des données sur. CloudWatch

Le rôle AWSServiceRoleForrePostPrivate lié à un service fait confiance aux services suivants pour assumer le rôle :

- `repostspace.amazonaws.com`

La politique d'autorisation de rôle nommée `AWSrePostPrivateCloudWatchAccess` permet à re:Post Private d'effectuer les actions suivantes sur les ressources spécifiées :

- Action sur `cloudwatch` : `PutMetricData`

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

Pour plus d'informations, consultez AWSrePostPrivateCloudWatchAccess.

Création d'un rôle lié à un service pour Re:Post Private

Vous n’avez pas besoin de créer manuellement un rôle lié à un service. Lorsque vous créez votre premier rôle privé Re:POST dans l'API AWS Management Console, le ou l' AWS API AWS CLI, Re:Post Private crée le rôle lié au service pour vous.

> **Important**
>
> Ce rôle lié à un service peut apparaître dans votre compte si vous avez effectué une action dans un autre service qui utilise les fonctions prises en charge par ce rôle. De plus, si vous utilisiez le service Re:Post Private avant le 1er décembre 2023, date à laquelle il a commencé à prendre en charge les rôles liés au service, Re:Post Private a créé le rôle dans votre compte. `AWSServiceRoleForrePostPrivate` Pour en savoir plus, voir Un nouveau rôle est apparu dans mon Compte AWS.

Si vous supprimez ce rôle lié à un service et que vous avez ensuite besoin de le recréer, vous pouvez utiliser la même procédure pour recréer le rôle dans votre compte. Lorsque vous créez votre premier rôle privé Re:post, Re:Post Private crée à nouveau le rôle lié au service pour vous.

Dans l'API AWS CLI ou dans l' AWS API, créez un rôle lié à un service avec le nom du `repostspace.amazonaws.com` service. Pour plus d’informations, consultez Création d’un rôle lié à un service dans le Guide de l’utilisateur IAM. Si vous supprimez ce rôle lié à un service, vous pouvez utiliser ce même processus pour créer le rôle à nouveau.

Modification d'un rôle lié à un service pour Re:Post Private

RE:Post Private ne vous permet pas de modifier le rôle lié au `AWSServiceRoleForrePostPrivate` service. Une fois que vous avez créé un rôle lié à un service, vous ne pouvez pas changer le nom du rôle, car plusieurs entités peuvent faire référence au rôle. Néanmoins, vous pouvez modifier la description du rôle à l’aide d’IAM. Pour plus d’informations, consultez Modification d’un rôle lié à un service dans le guide de l’utilisateur IAM.

Supprimer un rôle lié à un service pour Re:Post Private

Vous n'avez pas besoin de supprimer manuellement le rôle `AWSServiceRoleForrePostPrivate`. Lorsque vous supprimez votre Re:post privé dans l'API AWS Management Console, le ou l' AWS API AWS CLI, Re:Post Private supprime le rôle lié au service pour vous.

Vous pouvez également utiliser la console IAM, le AWS CLI, ou l' AWS API pour supprimer manuellement le rôle lié à un service.

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

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

Régions prises en charge pour les rôles liés au service Re:Post Private

Re:post Private prend en charge l'utilisation de rôles liés au service dans les AWS régions où le service est disponible.

Nom de la région	Identité de la région	Support dans Re:Post Private
US East (Virginie du Nord)	us-east-1	Oui
USA Est (Ohio)	us-east-2	Non
USA Ouest (Californie du Nord)	us-west-1	Non
USA Ouest (Oregon)	us-west-2	Oui
Afrique (Le Cap)	af-south-1	Non
Asie-Pacifique (Hong Kong)	ap-east-1	Non
Asie-Pacifique (Jakarta)	ap-southeast-3	Non
Asie-Pacifique (Mumbai)	ap-south-1	Non
Asie-Pacifique (Osaka)	ap-northeast-3	Non
Asie-Pacifique (Séoul)	ap-northeast-2	Non
Asie-Pacifique (Singapour)	ap-southeast-1	Oui
Asie-Pacifique (Sydney)	ap-southeast-2	Oui
Asie-Pacifique (Tokyo)	ap-northeast-1	Non

Nom de la région	Identité de la région	Support dans Re:Post Private
Canada (Centre)	ca-central-1	Oui
Europe (Francfort)	eu-central-1	Oui
Europe (Irlande)	eu-west-1	Oui
Europe (Londres)	eu-west-2	Non
Europe (Milan)	eu-south-1	Non
Europe (Paris)	eu-west-3	Non
Europe (Stockholm)	eu-north-1	Non
Moyen-Orient (Bahreïn)	me-south-1	Non
Moyen-Orient (EAU)	me-central-1	Non
Amérique du Sud (São Paulo)	sa-east-1	Non

Exemples de politiques basées sur l'identité privée AWS Re:POST

> **Note**
>
> Pour plus de sécurité, créez des utilisateurs fédérés plutôt que des utilisateurs IAM dans la mesure du possible.

Par défaut, AWS Identity and Access Management les utilisateurs et les rôles ne sont pas autorisés à créer ou à modifier des ressources AWS Re:POST Private. Ils ne peuvent pas non plus effectuer de tâches à l'aide de l' AWS API AWS Management Console AWS CLI, ou. Un administrateur IAM doit créer des politiques IAM autorisant les utilisateurs et les rôles à exécuter des opérations d'API spécifiques sur les ressources spécifiées dont ils ont besoin. Il doit ensuite attacher ces politiques aux utilisateurs ou aux groupes IAM ayant besoin de ces autorisations.

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

Rubriques

- Bonnes pratiques en matière de politiques
- Autorisation accordée aux utilisateurs pour afficher leurs propres autorisations

Bonnes pratiques en matière de politiques

Les politiques basées sur l'identité déterminent si quelqu'un peut créer, accéder ou supprimer des ressources Re:POST Private dans votre compte. Ces actions peuvent entraîner des frais pour votre Compte AWS. Lorsque vous créez ou modifiez des politiques basées sur l'identité, suivez ces instructions et recommandations :

- Commencez AWS par les politiques gérées et passez aux autorisations du moindre privilège : pour commencer à accorder des autorisations à vos utilisateurs et à vos charges de travail, utilisez les politiques AWS gérées qui accordent des autorisations pour de nombreux cas d'utilisation courants. Ils sont disponibles dans votre Compte AWS. Nous vous recommandons de réduire davantage les autorisations en définissant des politiques gérées par les AWS clients spécifiques à vos cas d'utilisation. Pour plus d'informations, consultez politiques gérées par AWS ou politiques gérées par AWS pour les activités professionnelles dans le Guide de l'utilisateur IAM.
- Accorder 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 de IAM pour appliquer des autorisations, consultez politiques et autorisations dans IAM dans le Guide de l'utilisateur IAM.
- Utiliser 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 AWS service, tel que AWS CloudFormation. Pour plus d'informations, consultez Conditions pour éléments de politique JSON IAM dans le Guide de l'utilisateur IAM.

- Utilisez IAM Access Analyzer pour valider vos politiques IAM afin de garantir des autorisations sécurisées et fonctionnelles : IAM Access Analyzer 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 politique 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 le MFA lorsque des opérations d'API sont appelées, ajoutez des conditions MFA à vos politiques. Pour plus d'informations, consultez Configuration de l'accès aux API protégé par 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.

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": "*"
        }
    ]
}
```

Politiques en ligne

Les politiques intégrées sont des politiques que vous créez et gérez. Vous pouvez intégrer des politiques intégrées directement dans un utilisateur, un groupe ou un rôle. Les exemples de politiques suivants montrent comment attribuer des autorisations pour effectuer des actions AWS re:POST Private. Pour obtenir des informations générales sur les politiques intégrées, consultez la section Gestion des politiques IAM dans le guide de l'utilisateur AWS IAM. Vous pouvez utiliser l' AWS Management Console interface de ligne de commande AWS Command Line Interface (CLI AWS) ou l' AWS Identity and Access Management API pour créer et intégrer des politiques en ligne.

Rubriques

- Accès en lecture seule à Re:Post Private
- Accès complet à Re:Post Private

Accès en lecture seule à Re:Post Private

La politique suivante accorde un accès en lecture à un utilisateur pour IAM Identity Center et la console Re:POST Private. Cette politique permet à l'utilisateur d'effectuer des actions Re:POST Private en lecture seule.

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

```
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "organizations:DescribeOrganization",
                "organizations:DescribeAccount",

                "sso:DescribeRegisteredRegions",
                "sso:ListDirectoryAssociations",
                "sso:GetSSOStatus",
                "sso:GetManagedApplicationInstance",
                "sso:ListProfiles",
                "sso:GetProfile",
                "sso:ListProfileAssociations",

                "sso-directory:DescribeDirectory",
                "sso-directory:SearchUsers",
                "sso-directory:SearchGroups",

                "repostspace:GetSpace",
                "repostspace:ListSpaces",
                "repostspace:ListTagsForResource"
            ],
            "Resource": "*"
        }
    ]
}
```

Accès complet à Re:Post Private

La politique suivante accorde à un utilisateur un accès complet à IAM Identity Center et à la console Re:POST Private. Cette politique permet à l'utilisateur d'effectuer toutes les actions Re:post Private.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "organizations:DescribeOrganization",
                "organizations:DescribeAccount",
```

```
                "sso:DescribeRegisteredRegions",
                "sso:ListDirectoryAssociations",
                "sso:GetSSOStatus",
                "sso:GetManagedApplicationInstance",
                "sso:ListProfiles",
                "sso:GetProfile",
                "sso:ListProfileAssociations",

                "sso:CreateManagedApplicationInstance",
                "sso:DeleteManagedApplicationInstance",
                "sso:AssociateProfile",
                "sso:DisassociateProfile",

                "sso-directory:DescribeDirectory",
                "sso-directory:SearchUsers",
                "sso-directory:SearchGroups",

                "kms:ListAliases",
                "kms:DescribeKey",
                "kms:CreateGrant",
                "kms:RetireGrant",

                "repostspace:*"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS politiques gérées pour AWS Re:Post Private

L'utilisation de politiques AWS gérées permet d'ajouter des autorisations aux utilisateurs, aux groupes et aux rôles plus facilement que de rédiger vous-même des politiques. Il faut du temps et de l'expertise pour créer des politiques gérées par le client IAM qui ne fournissent aux équipes que les autorisations dont elles ont besoin. Utilisez des politiques AWS gérées pour démarrer rapidement. Ces politiques couvrent les cas d'utilisation courants et sont disponibles dans votre AWS compte. Pour plus d'informations sur les politiques AWS gérées, voir les politiques AWS gérées dans le guide de l'utilisateur IAM.

AWS les services maintiennent et mettent à jour les politiques AWS gérées. Vous ne pouvez pas modifier les autorisations dans les politiques AWS gérées. Les services peuvent parfois ajouter des autorisations supplémentaires à une politique AWS gérée 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 plus susceptibles de mettre à jour une politique AWS gérée lorsqu'une nouvelle fonctionnalité est lancée ou lorsque de nouvelles opérations sont disponibles. Les services ne suppriment pas les autorisations d'une politique AWS gérée. Les mises à jour des politiques ne portent donc pas atteinte à vos autorisations existantes.

En outre, AWS prend en charge les politiques gérées pour les fonctions professionnelles qui couvrent plusieurs services. Par exemple, la politique `ReadOnlyAccess` AWS gérée fournit un accès en lecture seule à tous les AWS services et ressources. Lorsqu'un service lance une nouvelle fonctionnalité, il AWS ajoute des autorisations en lecture seule pour les nouvelles opérations et ressources. Pour plus d'informations, consultez la section Politiques gérées par AWS dans le Guide de l'utilisateur IAM.

Rubriques

- AWS politique gérée : AWSRepostSpaceSupportOperationsPolicy
- AWS politique gérée : AWSrePostPrivateCloudWatchAccess
- AWS Re:Post : Mises à jour privées des politiques gérées AWS

AWS politique gérée : AWSRepostSpaceSupportOperationsPolicy

Cette politique permet au service AWS Re:Post Private de créer, de gérer et de résoudre les AWS Support cas créés via l'application Web Re:Post Private.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "RepostSpaceSupportOperations",
   "Effect": "Allow",
   "Action": [
    "support:AddAttachmentsToSet",
    "support:AddCommunicationToCase",
    "support:CreateCase",
    "support:DescribeCases",
    "support:DescribeCommunications",
    "support:ResolveCase"
```

```
    ],
    "Resource": "*"
   }
  ]
}
```

AWS politique gérée : AWSrePostPrivateCloudWatchAccess

Cette politique permet au service Re:Post Private de publier des données sur. CloudWatch

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "CloudWatchPublishMetrics",
   "Effect": "Allow",
   "Action": [
    "cloudwatch:PutMetricData"
   ],
   "Resource": "*",
   "Condition": {
    "StringEquals": {
     "cloudwatch:namespace": [
      "AWS/rePostPrivate",
      "AWS/Usage"
     ]
    }
   }
  }
 ]
}
```

AWS Re:Post : Mises à jour privées des politiques gérées AWS

Consultez les détails des mises à jour des politiques AWS gérées pour Re:Post Private depuis que ce service a commencé à suivre ces modifications. Pour obtenir des alertes automatiques sur les modifications apportées à cette page, abonnez-vous au flux RSS de la page Historique du document.

Le tableau suivant décrit les mises à jour importantes apportées aux politiques gérées par Re:POST Private depuis le 26 novembre 2023.

Modification	Description	Date
Nouvelle politique - AWSrePostPrivateCloudWatchAccess	Nouvelle politique gérée pour la publication de données sur CloudWatch	26 novembre 2023
Nouvelle politique - AWSRepostSpaceSupportOperationsPolicy	Nouvelle politique gérée pour la fonctionnalité AWS Support dans AWS re:Post Private	26 novembre 2023
Re:Post Private a commencé à suivre les modifications	Re:Post Private a commencé à suivre les modifications apportées à ses politiques gérées AWS	26 novembre 2023

Résolution des problèmes liés à l'identité et à l'accès privés d'AWS re:POST

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

Rubriques

- Je ne suis pas autorisé à effectuer une action dans Re:Post Private
- Je ne suis pas autorisé à effectuer iam : PassRole
- Je souhaite permettre à des personnes extérieures Compte AWS à moi d'accéder à mes ressources privées Re:post

Je ne suis pas autorisé à effectuer une action dans Re:Post Private

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

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

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

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

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

Je ne suis pas autorisé à effectuer iam : PassRole

Si vous recevez un message d'erreur indiquant que vous n'êtes pas autorisé à effectuer l'`iam:PassRole`action, vos politiques doivent être mises à jour pour vous permettre de transmettre un rôle à re:Post Private.

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

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

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

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

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

Je souhaite permettre à des personnes extérieures Compte AWS à moi d'accéder à mes ressources privées Re:post

Vous pouvez créer un rôle que les utilisateurs provenant d'autres comptes ou les personnes extérieures à votre organisation pourront utiliser pour accéder à vos ressources. Vous pouvez

spécifier qui est autorisé à assumer le rôle. Pour les services qui prennent en charge les politiques basées sur les ressources ou les listes de contrôle d'accès (ACL), vous pouvez utiliser ces politiques pour donner l'accès à vos ressources.

Pour en savoir plus, consultez les éléments suivants :

- Pour savoir si RE:Post Private prend en charge ces fonctionnalités, consultez. Comment Re:post Private fonctionne avec IAM
- Pour savoir comment fournir l'accès à vos ressources sur celles Comptes AWS que vous possédez, consultez la section Fournir l'accès à un utilisateur IAM dans un autre utilisateur Compte AWS que vous possédez dans le Guide de l'utilisateur IAM.
- Pour savoir comment fournir l'accès à vos ressources à des tiers Comptes AWS, consultez la section Fournir un accès à des ressources Comptes AWS détenues par des tiers dans le guide de l'utilisateur IAM.
- Pour savoir comment fournir un accès par le biais de la fédération d'identité, consultez Fournir un accès à des utilisateurs authentifiés en externe (fédération d'identité) dans le Guide de l'utilisateur IAM.
- Pour en savoir plus sur la différence entre l'utilisation des rôles et des politiques basées sur les ressources pour l'accès intercompte, consultez Accès intercompte aux ressources dans IAM dans le Guide de l'utilisateur IAM.

Validation de conformité pour AWS Re:Post Private

Pour savoir si un programme AWS services de conformité AWS service s'inscrit dans le champ d'application de programmes de conformité spécifiques, consultez AWS services la section de conformité et sélectionnez le programme de conformité qui vous intéresse. Pour des informations générales, voir Programmes de AWS conformité Programmes AWS de .

Vous pouvez télécharger des rapports d'audit tiers à l'aide de AWS Artifact. Pour plus d'informations, voir Téléchargement de rapports dans AWS Artifact .

Votre responsabilité en matière de conformité lors de l'utilisation AWS services 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 : ces guides de déploiement abordent les considérations architecturales et fournissent des étapes pour déployer des environnements de base axés sur AWS la sécurité et la conformité.
- Architecture axée sur la sécurité et la conformité HIPAA sur Amazon Web Services : ce livre blanc décrit comment les entreprises peuvent créer des applications AWS conformes à la loi HIPAA.

> **Note**
>
> Tous ne AWS services sont pas éligibles à la loi HIPAA. Pour plus d'informations, consultez le HIPAA Eligible Services Reference.

- AWS Ressources de https://aws.amazon.com/compliance/resources/ de conformité — Cette collection de classeurs et de guides peut s'appliquer à votre secteur d'activité et à votre région.
- AWS Guides de conformité destinés aux clients — Comprenez le modèle de responsabilité partagée sous l'angle de la conformité. Les guides résument les meilleures pratiques en matière de sécurisation AWS services et décrivent les directives relatives aux contrôles de sécurité dans plusieurs cadres (notamment le National Institute of Standards and Technology (NIST), le Payment Card Industry Security Standards Council (PCI) et l'Organisation internationale de normalisation (ISO)).
- Évaluation des ressources à l'aide des règles du guide du AWS Config développeur : le AWS Config service évalue dans quelle mesure les configurations de vos ressources sont conformes aux pratiques internes, aux directives du secteur et aux réglementations.
- AWS Security Hub— Cela AWS service fournit une vue complète de votre état de sécurité interne AWS. Security Hub utilise des contrôles de sécurité pour évaluer vos ressources AWS et vérifier votre conformité par rapport aux normes et aux bonnes pratiques du secteur de la sécurité. Pour obtenir la liste des services et des contrôles pris en charge, consultez Référence des contrôles Security Hub.
- Amazon GuardDuty — Cela AWS service détecte les menaces potentielles qui pèsent sur vos charges de travail Comptes AWS, vos conteneurs et vos données en surveillant votre environnement pour détecter toute activité suspecte et malveillante. GuardDuty peut vous aider à répondre à diverses exigences de conformité, telles que la norme PCI DSS, en répondant aux exigences de détection des intrusions imposées par certains cadres de conformité.
- AWS Audit Manager— Cela vous AWS service permet d'auditer en permanence votre AWS utilisation afin de simplifier la gestion des risques et la conformité aux réglementations et aux normes du secteur.

Résilience dans AWS Re:Post Private

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.

Sécurité de l'infrastructure dans AWS Re:Post Private

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

Vous utilisez des appels d'API AWS publiés pour accéder à Re:Post Private via le réseau. Les clients doivent supporter le protocole TLS (Sécurité de la couche transport) 1.0 ou une version ultérieure. Nous recommandons TLS 1.2 ou version ultérieure. Les clients doivent aussi prendre en charge les suites de chiffrement PFS (Perfect Forward Secrecy) comme DHE (Ephemeral Diffie-Hellman) ou ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). La plupart des systèmes modernes tels que Java 7 et les versions ultérieures prennent en charge ces modes.

En outre, les demandes doivent être signées à l'aide d'un identifiant de clé d'accès et d'une clé d'accès secrète associés à un AWS Identity and Access Management principal. Vous pouvez également utiliser AWS Security Token Service (AWS STS) pour générer des informations d'identification de sécurité temporaires et signer les demandes.

Re:Post : quotas privés

AWS Re:Post Private fournit des Re:posts privés que vous pouvez utiliser sur votre compte dans une région donnée. AWS Lorsque vous vous inscrivez à Re:Post Private, AWS définit des quotas par défaut (anciennement appelés limites) sur le nombre de RE:Posts privés que vous pouvez créer et sur la taille des RE:Posts privés.

Service Quotas

Les quotas par défaut de Re:Post Private pour votre AWS compte sont les suivants. Vous pouvez utiliser la console Service Quotas pour consulter le quota par défaut. Aucun de ces quotas n'est ajustable. Vous ne pouvez pas demander d'augmentation de quota.

Ressource	Par défaut	Description	Ajustable
Nombre de Re:posts privés	3	Le nombre maximum de Re:posts privés sur ce compte dans la région actuelle.	Non
Format Re:post privé gratuit	10	La taille maximale (en Go) d'un Re:post privé gratuit.	Non
Taille privée standard : Re:post	100	La taille maximale (en Go) d'un Re:post privé standard.	Non

Limites de limitation de l'API

Les limites de limitation suivantes s'appliquent par compte et par région dans Re:post Private. Ces quotas ne peuvent pas être augmentés.

Actions	Taux de recharge des jetons	Taux de demandes	
CreateSpace	1	1	
ListSpaces	10	10	
GetSpace	10	10	
UpdateSpace	10	10	
DeleteSpace	1	1	
RegisterAdmin	10	100	
DeRegisterAdmin	10	100	
SendInvites	1	1	
TagResource	10	10	
UnTagResource	10	10	
ListTagsForResource	10	10	

Créez, configurez et personnalisez votre Re:Post privé

Rubriques

Créez un nouveau Re:Post privé

Pour créer un nouveau Re:Post privé, procédez comme suit :

1. Ouvrez la console Re:POST Private à l'adresse https://console.aws.amazon.com/repost-private/.
2. Sur la page d'accueil de la console, choisissez Create private Re:post.
3. Si IAM Identity Center n'est pas encore configuré pour votre compte, choisissez Open Identity Center. Suivez les instructions de la section Getting started du guide de l'utilisateur d'AWS IAM Identity Center.
4. Sur la page Create private Re:Post, pour la tarification, sélectionnez le niveau gratuit ou le niveau standard en fonction de votre cas d'utilisation. Si vous avez déjà utilisé le niveau gratuit pour votre compte, l'option niveau gratuit n'est pas disponible pour vous.
5. Sous Détails, procédez comme suit :

   Dans Nom, entrez un nom unique pour votre Re:Post privé.

   (Facultatif) Dans Description, entrez une brève description de votre Re:post privé.

   Pour Sous-domaine personnalisé, entrez un nom personnalisé pour votre sous-domaine.
6. (Facultatif) Pour personnaliser les paramètres de chiffrement des données, sous Chiffrement des données, sélectionnez Personnaliser les paramètres de chiffrement. Effectuez ensuite l'une des actions suivantes :

   Pour Choisir une clé AWS KMS, sélectionnez une AWS Key Management Service clé ou un Amazon Resource Name (ARN).

-ou-

Choisissez Créer une clé AWS KMS. Créez ensuite la AWS KMS clé.

7. (Facultatif) Sous Accès au service pour l'intégration des dossiers de support, sélectionnez Activer l'accès au service pour ce Re:Post.

> **Note**
>
> Vous pouvez également activer cette option après avoir créé le Re:post privé.

Pour Veuillez sélectionner un rôle IAM existant ci-dessous ou créer un nouveau rôle dans la console IAM, utilisez la barre de recherche pour trouver votre rôle IAM existant.

-ou-

Choisissez créer un nouveau rôle dans la console IAM.

Si vous choisissez de créer un nouveau rôle, suivez les instructions figurant dansCréer un rôle IAM.

Si vous choisissez d'utiliser un rôle de service existant, entrez l'ARN du rôle que vous souhaitez utiliser dans la barre de recherche. Choisissez le rôle dans la liste déroulante.

Pour plus d'informations, consultez Gestion de l'accès à AWS Support la création et à la gestion des dossiers dans Re:Post Private.

8. (Facultatif) Sous Balises, choisissez Ajouter une nouvelle étiquette. Entrez ensuite les informations suivantes :

Pour Key, entrez votre clé de tag personnalisée.

Dans Valeur, entrez la valeur de votre balise personnalisée.

Pour ajouter d'autres balises, choisissez Ajouter une nouvelle étiquette.

9. Choisissez Create this Re:Post.

Une page de confirmation vous indiquera que votre Re:Post privé est en cours de création. Vous pouvez consulter le statut du Re:post privé dans le champ Status. Lorsque votre Re:Post privé est créé, le champ Status affiche Creating.

La création du Re:post privé prend environ 30 minutes. Lorsque votre Re:post privé est prêt, le champ Status s'affiche En ligne. Vous pouvez utiliser le sous-domaine généré par AWS pour votre Re:Post privé répertorié sous l'onglet Paramètres pour accéder à votre Re:Post privé. Vous pouvez consulter le sous-domaine personnalisé de votre Re:Post privé sous l'onglet Paramètres une fois la révision terminée.

Gestion de l'accès à AWS Support la création et à la gestion des dossiers dans Re:Post Private

Vous devez créer un rôle AWS Identity and Access Management (IAM) pour gérer l'accès à la création et à AWS Support la gestion des dossiers depuis AWS Re:Post Private. Ce rôle exécute les AWS Support actions suivantes pour vous :

- CreateCase
- AddCommunicationToCase
- ResolveCase

Après avoir créé le rôle IAM, associez une politique IAM à ce rôle afin que le rôle dispose des autorisations requises pour effectuer ces actions. Vous choisissez ce rôle lorsque vous créez votre Re:POST privé dans la console Re:Post Private.

Les utilisateurs de votre Re:Post privé disposent des mêmes autorisations que celles que vous accordez au rôle IAM.

> **Important**
>
> Si vous modifiez le rôle ou la politique IAM, vos modifications s'appliquent au Re:POST privé que vous avez configuré.

Suivez ces procédures pour créer votre rôle et votre politique IAM.

Rubriques

Utiliser une politique AWS gérée ou créer une politique gérée par le client

Pour accorder des autorisations à votre rôle, vous pouvez utiliser une politique AWS gérée ou une politique gérée par le client.

> **Tip**
>
> Si vous ne souhaitez pas créer de stratégie manuellement, nous vous recommandons d'utiliser plutôt une stratégie AWS gérée et d'ignorer cette procédure. Les politiques gérées disposent automatiquement des autorisations requises pour AWS Support. Vous n'avez pas besoin de mettre à jour les politiques manuellement. Pour plus d'informations, consultez AWS politique gérée : AWSRepostSpaceSupportOperationsPolicy.

Suivez cette procédure pour créer une politique gérée par le client pour votre rôle. Cette procédure utilise l'éditeur de politique JSON dans la console IAM.

Pour créer une politique gérée par le client pour Re:Post Private

1. Connectez-vous à la console IAM AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/iam/.
2. Dans le panneau de navigation, choisissez Politiques.
3. Sélectionnez Create policy (Créer une politique).
4. Choisissez l'onglet JSON.
5. Saisissez votre JSON, puis remplacez le JSON par défaut dans l'éditeur. Vous pouvez utiliser l'exemple de politique.
6. Choisissez Suivant : Balises.
7. (Facultatif) Vous pouvez utiliser des balises comme paires clé-valeur pour ajouter des métadonnées à la politique.
8. Choisissez Suivant : vérification.

9. Dans la page Review policy (Vérifier la politique), saisissez un Name (Nom), tel que *rePostPrivateSupportPolicy*, et une Description (facultatif).
10. Consultez la page Résumé pour voir les autorisations autorisées par la politique, puis choisissez Créer une politique.

Cette politique définit les actions que le rôle peut prendre. Pour plus d'informations, consultez Création de politiques IAM (console) dans le Guide de l'utilisateur IAM.

Exemple de politique IAM

Vous pouvez associer l'exemple de politique suivant à votre rôle IAM. Cette politique permet au rôle de disposer d'autorisations complètes pour toutes les actions requises pour AWS Support. Une fois que vous avez configuré un Re:Post privé avec le rôle, tous les utilisateurs de votre Re:Post privé ont les mêmes autorisations.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "RepostSpaceSupportOperations",
   "Effect": "Allow",
   "Action": [
    "support:AddAttachmentsToSet",
    "support:AddCommunicationToCase",
    "support:CreateCase",
    "support:DescribeCases",
    "support:DescribeCommunications",
    "support:ResolveCase"
   ],
   "Resource": "*"
  }
 ]
}
```

> **Note**
>
> Pour obtenir la liste des politiques AWS gérées pour Re:Post Private, consultez. AWS politiques gérées pour AWS Re:Post Private

Vous pouvez mettre à jour la politique pour supprimer une autorisation de AWS Support.

Pour obtenir des descriptions de chaque action, consultez les rubriques suivantes dans la référence de l'autorisation de service :

- Actions, ressources et clés de condition pour AWS Support
- Actions, ressources et clés de condition pour Service Quotas
- Actions, ressources et clés de condition pour AWS Identity and Access Management

Créer un rôle IAM

Après avoir créé la politique, vous devez créer un rôle IAM, puis associer la politique à ce rôle. Vous choisissez ce rôle lorsque vous créez un Re:POST privé dans la console Re:Post Private.

Pour créer un rôle pour la AWS Support création et la gestion des dossiers

1. Connectez-vous à la console IAM AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/iam/.
2. Dans le volet de navigation, sélectionnez Rôles, puis Créer un rôle.
3. Pour Trusted entity type (Type d'entité de confiance), choisissez Custom trust policy (Politique de confiance personnalisée).
4. Pour la politique de confiance personnalisée, entrez ce qui suit :

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

5. Choisissez Suivant.

6. Sous Politiques d'autorisations, dans la barre de recherche, entrez la politique AWS gérée ou une politique gérée par le client que vous avez créée, telle que *rePostPrivateSupportPolicy*. Cochez la case située à côté des politiques d'autorisation que vous souhaitez attribuer au service.
7. Choisissez Suivant.
8. Sur la page Nom, révision et création, pour Nom du rôle, entrez un nom, tel que *rePostPrivateSupportRole*.
9. (Facultatif) Dans Description, entrez une description pour le rôle.
10. Passez en revue la politique de confiance et les autorisations.
11. (Facultatif) Vous pouvez utiliser des balises comme paires clé-valeur pour ajouter des métadonnées au rôle. Pour plus d'informations sur l'utilisation de balises dans IAM, consultez Balisage des ressources IAM.
12. Sélectionnez Créer un rôle. Vous pouvez désormais choisir ce rôle lorsque vous configurez un Re:POST privé dans la console Re:Post Private. veuillez consulter Créez un nouveau Re:Post privé.

Pour plus d'informations, consultez la section Création d'un rôle pour un AWS service (console) dans le guide de l'utilisateur IAM.

Résolution des problèmes

Consultez les rubriques suivantes pour gérer l'accès à re:Post Private.

Table des matières

Je souhaite empêcher certains utilisateurs de mon Re:post privé d'effectuer des actions spécifiques

Par défaut, les utilisateurs de votre Re:Post privé disposent des mêmes autorisations spécifiées dans la politique IAM que vous attachez au rôle IAM que vous créez. Cela signifie que tous les membres

du réseau privé Re:Post disposent d'un accès en lecture ou en écriture pour créer et gérer des AWS Support dossiers, qu'ils aient ou non un utilisateur IAM Compte AWS ou un utilisateur IAM.

Nous recommandons les bonnes pratiques suivantes :

- Utilisez une politique IAM dotée des autorisations minimales requises pour. AWS Support veuillez consulter AWS politique gérée : AWSRepostSpaceSupportOperationsPolicy.

Lorsque je configure un Re:POST privé, je ne vois pas le rôle IAM que j'ai créé

Si votre rôle IAM n'apparaît pas dans la liste des rôles IAM pour Re:post Private ;, cela signifie que Re:Post Private n'est pas une entité de confiance pour le rôle, ou que le rôle a été supprimé. Vous pouvez mettre à jour le rôle existant ou en créer un autre. veuillez consulter Créer un rôle IAM.

Il manque une autorisation à mon rôle IAM

Le rôle IAM que vous créez pour votre Re:Post privé nécessite des autorisations pour effectuer les actions que vous souhaitez. Par exemple, si vous souhaitez que les utilisateurs du réseau privé Re:Post créent des demandes d'assistance, le rôle doit disposer de l'`support:CreateCase`autorisation. Re:Post Private assume ce rôle pour effectuer ces actions à votre place.

Si vous recevez un message d'erreur concernant une autorisation manquante pour AWS Support, vérifiez que la politique associée à votre rôle dispose de l'autorisation requise.

Voir le Exemple de politique IAM précédent.

Une erreur indique que mon rôle IAM n'est pas valide

Vérifiez que vous avez choisi le bon rôle pour votre configuration privée Re:POST.

Configurez et gérez l'accès des utilisateurs à l'aide de AWS IAM Identity Center

Re:post Private s'intègre AWS IAM Identity Center pour fournir une fédération d'identité au personnel de votre organisation. Utilisez IAM Identity Center pour créer ou connecter des utilisateurs de votre organisation et gérer de manière centralisée leur accès à tous leurs AWS comptes et applications. Pour plus d'informations sur IAM Identity Center, consultez Qu'est-ce qu'AWS IAM Identity Center

(successeur d'AWS Single Sign-On). Pour plus d'informations sur la prise en main d'IAM Identity Center, consultez Getting started. Pour utiliser IAM Identity Center, vous devez également avoir AWS Organizations activé le compte.

Personnalisez votre Re:Post privé

Vous pouvez ajouter un ou plusieurs administrateurs à votre Re:post privé après l'avoir créé. Les administrateurs utilisent l'application Re:Post Private pour lancer le Re:POST privé et gérer les utilisateurs qu'il contient. Ils peuvent personnaliser l'image de marque du Re:post privé, ajouter des balises pour classer le contenu et sélectionner des sujets d'intérêt pour le peuplement automatique du contenu. Pour plus d'informations, consultez le guide d'administration privée d'AWS re:Post.

Invitez des utilisateurs à votre Re:Post privé

Vous pouvez ajouter un ou plusieurs utilisateurs à votre Re:Post privé après l'avoir créé. Vous pouvez inviter des utilisateurs à collaborer au sein de votre Re:Post privé. Les utilisateurs utilisent l'application Re:Post Private pour se connecter à l'aide des informations d'identification que vous avez configurées. Une fois connectés à un Re:post privé, les utilisateurs peuvent parcourir ou rechercher du contenu existant, y compris des formations personnalisées et du contenu technique adapté à leurs sujets d'intérêt. Pour plus d'informations, consultez le guide de l'utilisateur privé d'AWS re:Post.

Gérez votre Re:POST privé dans la console Re:Post Private

Cette section explique comment gérer votre Re:POST privé dans la console AWS Re:POST Private.

Rubriques

Ajoutez des utilisateurs et des groupes à votre Re:Post privé

Si vous êtes administrateur, vous pouvez ajouter des utilisateurs et des groupes à votre Re:Post privé.

Ajoutez des utilisateurs à votre Re:Post privé

1. Ouvrez la console Re:POST Private à l'adresse https://console.aws.amazon.com/repost-private/.
2. Dans le volet de navigation, choisissez All my private Re:Posts.
3. Choisissez le Re:Post privé que vous souhaitez gérer.
4. Sélectionnez l'onglet Utilisateurs.
5. Sous Utilisateurs, sélectionnez Ajouter des utilisateurs et des groupes.
6. Dans la liste, sélectionnez les utilisateurs que vous souhaitez ajouter à votre Re:Post privé. Choisissez ensuite Attribuer.

Les utilisateurs sélectionnés sont ajoutés à votre Re:Post privé et répertoriés sous l'onglet Utilisateurs.

Ajoutez des groupes à votre Re:Post privé

1. Ouvrez la console Re:POST Private à l'adresse https://console.aws.amazon.com/repost-private/.

2. Dans le volet de navigation, choisissez All my private Re:Posts.
3. Choisissez le Re:Post privé que vous souhaitez gérer.
4. Cliquez sur l'onglet Groups (Groupes).
5. Choisissez Ajouter des utilisateurs et des groupes.
6. Dans la liste, sélectionnez les groupes que vous souhaitez ajouter à votre Re:Post privé. Choisissez ensuite Attribuer.

Les groupes sélectionnés sont ajoutés à votre Re:post privé et répertoriés sous l'onglet Groupes.

Ajoutez des utilisateurs à un groupe dans votre Re:Post privé

Utilisez IAM Identity Center pour ajouter de nouveaux utilisateurs à un groupe existant dans votre Re:Post privé. Pour plus d'informations, consultez la section Ajouter des utilisateurs à des groupes dans le guide de l'utilisateur d'AWS IAM Identity Center.

Invitez des utilisateurs et des groupes à votre Re:Post privé

Suivez ces étapes pour inviter des utilisateurs et des groupes à rejoindre votre Re:Post privé dans AWS Re:Post Private :

1. Ouvrez la console Re:POST Private à l'adresse https://console.aws.amazon.com/repost-private/.
2. Dans le volet de navigation, choisissez All my private Re:Posts.
3. Choisissez le Re:Post privé que vous souhaitez gérer.
4. Pour inviter des utilisateurs à votre Re:post privé, cliquez sur l'onglet Utilisateurs.

   Dans la liste, sélectionnez les utilisateurs que vous souhaitez inviter à votre Re:Post privé. Choisissez ensuite Onboard users to Re:post.
5. Dans la boîte de dialogue Intégrer les utilisateurs à ce Re:POST privé, entrez les informations suivantes :

   Dans le champ Objet, saisissez l'objet du message électronique que vous envoyez.

   Pour Body, entrez un message de bienvenue pour votre Re:post privé.

   Choisissez Envoyer un e-mail d'intégration.
6. Pour inviter des groupes à rejoindre votre Re:post privé, cliquez sur l'onglet Groupes.

Dans la liste, sélectionnez les groupes que vous souhaitez inviter à votre Re:post privé. Ensuite, choisissez Onboard groups to Re:post.

7. Dans la boîte de dialogue Intégrer les groupes à cette boîte de dialogue privée Re:POST, entrez les informations suivantes :

   Dans le champ Objet, saisissez l'objet du message électronique que vous envoyez.

   Pour Body, entrez un message de bienvenue pour votre Re:post privé.

   Choisissez Envoyer un e-mail d'intégration.

Le message de bienvenue est envoyé à tous les utilisateurs et groupes sélectionnés avec des informations sur la manière de se connecter à votre Re:Post privé.

Promouvez un utilisateur dans votre compte Re:post privé auprès de l'administrateur

Pour promouvoir un utilisateur privé de Re:post au rang d'administrateur, procédez comme suit :

1. Ouvrez la console Re:POST Private à l'adresse https://console.aws.amazon.com/repost-private/.
2. Dans le volet de navigation, choisissez All my private Re:Posts.
3. Choisissez le Re:Post privé que vous souhaitez gérer.
4. Sélectionnez l'onglet Utilisateurs.
5. Sélectionnez un ou plusieurs utilisateurs que vous souhaitez promouvoir au poste d'administrateur.
6. Choisissez Modifier le rôle, puis choisissez Make admin.

Les utilisateurs sélectionnés sont promus administrateurs. Dans l'onglet Utilisateurs, le rôle de ces utilisateurs est mis à jour en tant qu'administrateur.

Supprimer des utilisateurs ou des groupes de votre Re:Post privé

Si vous êtes administrateur, vous pouvez supprimer des utilisateurs ou des groupes de votre Re:Post privé.

Supprimer des utilisateurs de votre Re:Post privé

1. Ouvrez la console Re:POST Private à l'adresse https://console.aws.amazon.com/repost-private/.
2. Dans le volet de navigation, choisissez All my private Re:Posts.
3. Choisissez le Re:Post privé que vous souhaitez gérer.
4. Sous Utilisateurs, dans la liste, sélectionnez les utilisateurs que vous souhaitez supprimer de votre Re:Post privé. Choisissez ensuite Supprimer.

Les utilisateurs sélectionnés sont supprimés de votre Re:Post privé. Les informations relatives aux utilisateurs supprimés n'apparaissent plus sous l'onglet Utilisateurs.

Supprimer des groupes de votre Re:Post privé

1. Ouvrez la console Re:POST Private à l'adresse https://console.aws.amazon.com/repost-private/.
2. Dans le volet de navigation, choisissez All my private Re:Posts.
3. Choisissez le Re:Post privé que vous souhaitez gérer.
4. Cliquez sur l'onglet Groups (Groupes).
5. Dans la liste, sélectionnez les groupes que vous souhaitez supprimer de votre Re:Post privé. Choisissez ensuite Supprimer.

Les groupes sélectionnés sont supprimés de votre Re:Post privé. Les informations relatives aux groupes supprimés n'apparaissent plus sous l'onglet Groupes.

Ajouter ou supprimer un AWS employé de votre Re:Post privé

Si vous disposez d'un plan de support Enterprise ou Enterprise On-Ramp, vous pouvez ajouter ou supprimer un employé AWS de votre Re:Post privé. Contactez le support de conciergerie ou votre responsable de compte technique (TAM) pour plus d'informations.

Supprimer un Re:Post privé de Re:Post Private

Pour supprimer un Re:Post privé dans AWS Re:Post Private, procédez comme suit :

1. Ouvrez la console Re:POST Private à l'adresse https://console.aws.amazon.com/repost-private/.
2. Dans le volet de navigation, choisissez All my private Re:Posts.
3. Choisissez le Re:Post privé que vous souhaitez gérer, puis choisissez Supprimer.

4. Sélectionnez toutes les options pour confirmer que vous souhaitez supprimer définitivement le fichier privé Re:post et les données qui y sont associées.

> **⚠ Important**
>
> Lorsque vous supprimez le Re:Post privé, toutes les informations de configuration associées au Re:Post privé sont supprimées. Une fois le Re:post privé supprimé, vous ne pouvez plus en restaurer le contenu.

5. Entrez le nom de votre Re:post privé lorsque vous êtes invité à obtenir un consentement écrit supplémentaire. Ensuite, choisissez Supprimer.

La suppression de votre Re:Post privé prend environ 30 minutes.

Surveillance d'AWS Re:Post Private

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

- Amazon CloudWatch surveille vos AWS ressources et les applications que vous utilisez AWS en temps réel. Vous pouvez collecter et suivre les métriques, créer des tableaux de bord personnalisés, et définir des alarmes qui vous informent ou prennent des mesures lorsqu'une métrique spécifique atteint un seuil que vous spécifiez. Par exemple, vous pouvez CloudWatch suivre l'utilisation du processeur ou d'autres indicateurs de vos instances Amazon EC2 et lancer automatiquement de nouvelles instances en cas de besoin. Pour plus d'informations, consultez le guide de CloudWatch l'utilisateur Amazon.
- AWS CloudTrailcapture les appels d'API et les événements associés effectués par ou pour vous Compte AWS et envoie les fichiers journaux dans un compartiment Amazon S3 que vous spécifiez. Vous pouvez identifier les utilisateurs et les comptes qui ont appelé AWS, l'adresse IP source à partir de laquelle les appels ont été émis, ainsi que le moment où les appels ont eu lieu. Pour de plus amples informations, veuillez consulter le Guide de l'utilisateur AWS CloudTrail.

Surveillance d'AWS Re:Post Private avec Amazon CloudWatch

Vous pouvez surveiller AWS Re:Post Private à l'aide d'Amazon CloudWatch, qui collecte les données brutes et les traite pour en faire des métriques lisibles en temps quasi réel. Ces statistiques sont conservées pendant 15 mois afin que vous puissiez accéder aux informations historiques et avoir une meilleure idée des performances de votre application ou service Web. Vous pouvez également définir des alarmes qui surveillent certains seuils et envoient des notifications ou prennent des mesures lorsque ces seuils sont atteints. Pour plus d'informations, consultez le guide de CloudWatch l'utilisateur Amazon.

Le service Re:post Private indique les métriques suivantes dans l'espace de `AWS/rePostPrivate` noms.

Métrique	Description
`NumberOfSpaces`	Le nombre de Re:posts privés sur le compte courant.

Métrique	Description
	Unités : nombre
`NumberOfUsers`	Le nombre d'utilisateurs d'un Re:post privé. Cette métrique utilise SpaceID comme dimension. Unités : nombre
`ContentSize`	La quantité de contenu d'un Re:post privé. Cette métrique utilise SpaceID comme dimension. Unités : octets

Les dimensions suivantes sont prises en charge pour les métriques Re:Post Private.

Dimension	Description
`spaceId`	L'identifiant unique du Re:post privé.

Journalisation des appels d'API privés AWS Re:POST à l'aide de AWS CloudTrail

AWS Re:Post Private est intégré à AWS CloudTrail un service qui fournit un enregistrement des actions effectuées par un utilisateur, un rôle ou un AWS service dans Re:Post Private. CloudTrail capture tous les appels d'API pour Re:Post Private sous forme d'événements. Les appels capturés incluent des appels provenant de la console Re:Post Private et des appels de code vers les opérations de l'API Re:POST Private. Si vous créez un suivi, vous pouvez activer la diffusion continue des CloudTrail événements vers un compartiment Amazon S3, y compris des événements pour Re:Post Private. 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 Re:Post Private, 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.

Re:Publier des informations privées dans CloudTrail

CloudTrail est activé sur votre compte Compte AWS lorsque vous créez le compte. Lorsqu'une activité se produit dans Re:post Private, 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 Utilisation de l'historique des CloudTrail événements.

Pour un enregistrement continu des événements de votre siteCompte AWS, y compris ceux de Re:post Private, 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 d'activité consigne les événements de toutes les Régions dans la partition AWS et livre les fichiers journaux dans le compartiment Simple Storage Service (Amazon S3) de votre choix. 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 :

- Création d'un journal de suivi pour votre compte AWS
- 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 Re:Post Private sont enregistrées CloudTrail et documentées dans le document AWS Re:POST Private API Reference. Re:Post Private prend en charge la journalisation des actions suivantes sous forme d'événements dans les fichiers journaux : CloudTrail

- CreateSpace
- DeleteSpace
- DeregisterAdmin
- GetSpace
- ListSpaces
- ListTagsForResource
- RegisterAdmin
- SendInvites

- TagResource
- UntagResource
- UpdateSpace

RE:Post Private prend en charge l'enregistrement des AWS Support actions suivantes sous forme d'événements dans les fichiers CloudTrail journaux :

- CreateCase
- AddCommunicationToCase
- ResolveCase

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 effectuée avec les informations d'identification utilisateur racine ou AWS Identity and Access Management (IAM).
- Si la demande a été effectuée avec les informations d'identification de sécurité temporaires d'un rôle ou d'un utilisateur fédéré.
- Si la requête a été effectuée par un autre service AWS.

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

Comprendre les entrées du fichier journal privé Re:POST

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'`CreateSpace`action.

```
{
   "eventVersion": "1.08",
```

```
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAQM47QIR7WLEXAMPLE:user",
        "arn": "arn:aws:sts::123456789012:assumed-role/User/user",
        "accountId": "123456789012",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAQM47QIR7WLEXAMPLE",
                "arn": "arn:aws:iam::123456789012:role/User",
                "accountId": "123456789012",
                "userName": "User"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-11-06T19:24:39Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-11-06T21:37:44Z",
    "eventSource": "repostspace.amazonaws.com",
    "eventName": "CreateSpace",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "205.251.233.176",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/118.0.0.0 Safari/537.36",
    "requestParameters": {
        "spaceName": "Test space name",
        "spaceSubdomain": "customsubdomain",
        "tagSet": {},
        "tier": "2000",
        "roleArn": "",
        "spaceDescription": "Test space description"
    },
    "responseElements": {
        "spaceId": "SPLPWvQmv9SIWYF30EXAMPLE",
        "Access-Control-Expose-Headers": "x-amzn-errortype, x-amzn-requestid, x-amzn-
errormessage, x-amzn-trace-id, x-amz-apigw-id, date"
    },
    "requestID": "71d815e0-6632-4ec9-9fac-92af3e4a86dc",
    "eventID": "30a6c3da-ce2e-4931-ba5d-b3cc7cf16ec8",
    "readOnly": false,
```

```
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management"
}
```

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

```
{
   "eventVersion": "1.08",
   "userIdentity": {
       "type": "AssumedRole",
       "principalId": "AROAQM47QIR7WLEXAMPLE:user",
       "arn": "arn:aws:sts::123456789012:assumed-role/User/user",
       "accountId": "123456789012",
       "accessKeyId": "EXAMPLE_KEY_ID",
       "sessionContext": {
           "sessionIssuer": {
               "type": "Role",
               "principalId": "AROAQM47QIR7WLEXAMPLE",
               "arn": "arn:aws:iam::123456789012:role/User",
               "accountId": "123456789012",
               "userName": "User"
           },
           "webIdFederationData": {},
           "attributes": {
               "creationDate": "2023-11-07T21:17:19Z",
               "mfaAuthenticated": "false"
           }
       }
   },
   "eventTime": "2023-11-07T21:24:23Z",
   "eventSource": "repostspace.amazonaws.com",
   "eventName": "RegisterAdmin",
   "awsRegion": "us-west-2",
   "sourceIPAddress": "205.251.233.183",
   "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/118.0.0.0 Safari/537.36",
   "requestParameters": {
       "adminId": "08612310-a0f1-7063-3e54-fb2960444dd1",
       "spaceId": "SPlYNZE-ylQEmAXpmEXAMPLE"
```

```
    },
    "responseElements": {
        "Access-Control-Expose-Headers": "x-amzn-errortype, x-amzn-requestid, x-amzn-
errormessage, x-amzn-trace-id, x-amz-apigw-id, date"
    },
    "requestID": "9939ebbe-8599-4f9a-827b-4995e3006001",
    "eventID": "e1873b18-f80c-4934-9ff2-bf5b35c78031",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management"
}
```

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

```
 {
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAQM47QIR7WLEXAMPLE:user",
        "arn": "arn:aws:sts::123456789012:assumed-role/User/user",
        "accountId": "123456789012",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAQM47QIR7WLEXAMPLE",
                "arn": "arn:aws:iam::123456789012:role/User",
                "accountId": "123456789012",
                "userName": "User"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-11-09T22:28:23Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-11-09T22:38:34Z",
    "eventSource": "repostspace.amazonaws.com",
```

```
    "eventName": "ListSpaces",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "205.251.233.176",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36",
    "requestParameters": null,
    "responseElements": null,
    "requestID": "95be587b-c04f-4eb0-9269-12fee33ae2e3",
    "eventID": "9777da32-545f-44c4-af0b-1d9109b8cbc3",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management"
}
```

L'exemple suivant montre une entrée de CloudTrail journal illustrant l'`ResolveCase`action. Vous pouvez utiliser l'`sourceIdentity`élément de cette entrée de journal pour identifier l'utilisateur qui a résolu le problème.

```
 {
    "eventVersion": "1.09",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAQM47QIR76DQZ7N5WX:create-support-case-
Uk1iHNTWQEOLmR2BR1FDJQ",
        "arn": "arn:aws:sts::123456789012:assumed-role/AWSRepostSpaceRole/create-
support-case-Uk1iHNTWQEOLmR2BR1FDJQ",
        "accountId": "123456789012",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAQM47QIR76DQZ7N5WX",
                "arn": "arn:aws:iam::123456789012:role/AWSRepostSpaceRole",
                "accountId": "123456789012",
                "userName": "AWSRepostSpaceRole"
            },
            "attributes": {
                "creationDate": "2023-11-17T21:46:42Z",
                "mfaAuthenticated": "false"
            },
```

```
            "sourceIdentity": "28e17330-10f1-705d-7cba-3a62a6b10e2e"
        }
    },
    "eventTime": "2023-11-17T21:46:44Z",
    "eventSource": "support.amazonaws.com",
    "eventName": "ResolveCase",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "54.68.27.29",
    "userAgent": "aws-sdk-nodejs/2.1363.0 linux/v16.20.2 exec-env/AWS_ECS_FARGATE
 promise",
    "requestParameters": {
        "caseId": "case-123456789012-muen-2023-75d2c35481b96357"
    },
    "responseElements": {
        "initialCaseStatus": "unassigned",
        "finalCaseStatus": "resolved"
    },
    "requestID": "594b91c6-df1c-47e4-a834-d67d67f34b9d",
    "eventID": "7fc9cbe4-c8d5-4d61-a016-e076de272fff",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111111111111",
    "eventCategory": "Management",
    "tlsDetails": {
        "clientProvidedHostHeader": "support.us-west-2.amazonaws.com"
    }
}
```

Résolution des problèmes liés à Re:Post Private

Les informations suivantes peuvent vous aider à résoudre les problèmes liés à AWS re:Post Private.

Rubriques

Impossible de configurer mon Re:Post privé dans une région spécifique AWS

Re:post Private est disponible uniquement dans les régions USA Est (Virginie du Nord), USA Ouest (Oregon), Europe (Francfort), Asie-Pacifique (Singapour), Asie-Pacifique (Sydney), Canada (Centre) et Europe (Irlande). Assurez-vous de créer votre Re:post privé dans l'une de ces régions.

Impossible de configurer Re:Post en mode privé sur mon compte

Assurez-vous d'avoir activé votre compte et AWS IAM Identity Center d'avoir configuré IAM Identity Center dans la même région que celle dans laquelle vous souhaitez créer le Re:post privé. Pour plus d’informations, consultez Prérequis.

Impossible de gérer les utilisateurs ou les groupes dans un Re:Post privé

Assurez-vous de disposer des autorisations requises pour modifier un Re:Post privé et gérer les utilisateurs et les groupes au sein du Re:Post privé. Pour plus d'informations, voir Exemples de politiques basées sur l'identité privée AWS Re:POST.

Historique du document

Le tableau suivant décrit les versions de documentation d'AWS re:Post Private :

Modification	Description	Date
Mettre à jour	Ajout des États-Unis Est (Virginie du Nord), de l'Asie-Pacifique (Sydney), du Canada (Centre) et de l'Europe (Irlande) aux régions prises en charge	10 mai 2024
Mettre à jour	Ajout de l'Asie-Pacifique (Singapour) aux régions prises en charge	6 mars 2024
Nouvelles ressources	Ajout de documentation sur les politiques gérées par AWS pour AWS Re:Post Private	26 novembre 2023
Première version	Publication initiale du guide d'administration de la console privée Re:POST	26 novembre 2023

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.