Guide de l’utilisateur

AWS Sign-In

AWS Sign-In: Guide de l’utilisateur

Table of Contents

Qu'est-ce que AWS Sign-In?

Ce guide vous aide à comprendre les différentes manières de vous connecter à Amazon Web Services (AWS), en fonction du type d'utilisateur que vous êtes. Pour plus d'informations sur la procédure de connexion en fonction de votre type d'utilisateur et des AWS ressources auxquelles vous souhaitez accéder, consultez l'un des didacticiels suivants.

- Connectez-vous au AWS Management Console
- Connectez-vous à votre AWS portail d'accès
- Connectez-vous en tant qu'identité fédérée
- Connectez-vous via le AWS Command Line Interface
- Connectez-vous avec ID de constructeur AWS

Si vous rencontrez des problèmes pour vous connecter à votre Compte AWS, consultezRésolution des problèmes Compte AWS problèmes de connexion. Pour obtenir de l'aide concernant votre ID de constructeur AWS siègeRésolution des problèmes liés à AWS Builder ID. Vous cherchez à créer un Compte AWS ? Inscrivez-vous pour AWS. Pour plus d'informations sur la façon dont l'inscription AWS peut vous aider, vous ou votre organisation, voir Contactez-nous.

Rubriques

- Terminologie
- Disponibilité de la région pour AWS Sign-In
- Sign-in journalisation des événements
- Déterminez votre type d'utilisateur
- Déterminez votre URL de connexion
- Domaines à ajouter à votre liste d'autorisations
- Bonnes pratiques en matière de sécurité pour Compte AWS administrateurs

Terminologie

Amazon Web Services (AWS) utilise une terminologie courante pour décrire le processus de connexion. Nous vous recommandons de lire et de comprendre ces conditions.

Administrateur

Également appelé Compte AWS administrateur ou administrateur IAM. L'administrateur, généralement le personnel des technologies de l'information (TI), est une personne qui supervise un Compte AWS. Les administrateurs disposent d'un niveau d'autorisations supérieur à Compte AWS celui des autres membres de leur organisation. Les administrateurs établissent et mettent en œuvre les paramètres du Compte AWS. Ils créent également des utilisateurs IAM ou IAM Identity Center. L'administrateur fournit à ces utilisateurs leurs informations d'accès et une URL de connexion à laquelle se connecter AWS.

Compte

Une norme Compte AWS contient à la fois vos AWS ressources et les identités qui peuvent accéder à ces ressources. Les comptes sont associés à l'adresse e-mail et au mot de passe du propriétaire du compte.

Informations d'identification

Également appelés identifiants d'accès ou identifiants de sécurité. Dans l'authentification et l'autorisation, un système utilise les informations d'identification pour identifier la personne qui effectue l'appel et pour autoriser ou pas l'accès demandé. Les informations d'identification sont les informations que les utilisateurs fournissent AWS pour se connecter et accéder aux AWS ressources. Les informations d'identification des utilisateurs humains peuvent inclure une adresse e-mail, un nom d'utilisateur, un mot de passe défini par l'utilisateur, un identifiant ou un alias de compte, un code de vérification et un code d'authentification multifactorielle à usage unique (MFA). Pour l'accès par programmation, vous pouvez également utiliser les touches d'accès. Nous vous recommandons d'utiliser des clés d'accès à court terme si possible.

Pour plus d'informations sur les informations d'identification, consultez AWS la section Informations d'identification de sécurité.

> **Note**
>
> Le type d'informations d'identification qu'un utilisateur doit soumettre dépend de son type d'utilisateur.

Identifiants de l'entreprise

Les informations d'identification fournies par les utilisateurs lorsqu'ils accèdent au réseau et aux ressources de leur entreprise. L'administrateur de votre entreprise peut configurer votre compte Compte AWS pour utiliser les mêmes informations d'identification que celles que vous utilisez pour accéder au réseau et aux ressources de votre entreprise. Ces informations d'identification vous sont fournies par votre administrateur ou un employé du service d'assistance.

Profil

Lorsque vous vous inscrivez pour obtenir un AWS Builder ID, vous créez un profil. Votre profil inclut les informations de contact que vous avez fournies et la possibilité de gérer les appareils d'authentification multifactorielle (MFA) et les sessions actives. Vous pouvez également en savoir plus sur la confidentialité et la manière dont nous traitons vos données dans votre profil. Pour plus d'informations sur votre profil et son lien avec un Compte AWS, consultezID de constructeur AWS et autres AWS informations d'identification.

Informations d'identification de l'utilisateur root

Les informations d'identification de l'utilisateur root sont l'adresse e-mail et le mot de passe utilisés pour créer le Compte AWS. Nous recommandons vivement d'ajouter le MFA aux informations d'identification de l'utilisateur root pour plus de sécurité. Les informations d'identification de l'utilisateur root fournissent un accès complet à tous les AWS services et ressources du compte. Pour plus d'informations sur l'utilisateur root, consultezUtilisateur root.

Utilisateur

Un utilisateur est une personne ou une application autorisée à effectuer des appels d'API vers AWS des produits ou à accéder à AWS des ressources. Chaque utilisateur possède un ensemble unique d'informations de sécurité qui ne sont pas partagées avec d'autres utilisateurs. Ces informations d'identification sont distinctes des informations de sécurité pour Compte AWS. Pour de plus amples informations, veuillez consulter Déterminez votre type d'utilisateur.

Code de vérification

Un code de vérification vérifie votre identité lors du processus de connexion à l'aide de l'authentification multifactorielle (MFA). Les méthodes de livraison des codes de vérification varient. Ils peuvent être envoyés par SMS ou par e-mail. Consultez votre administrateur pour plus d'informations.

Disponibilité de la région pour AWS Sign-In

AWS Sign-in est disponible en plusieurs versions couramment utilisées Régions AWS. Cette disponibilité vous permet d'accéder plus facilement aux AWS services et aux applications métiers. Pour une liste complète des régions prises Sign-in en charge, consultez la section AWS Sign-In Points de terminaison et quotas.

Sign-in journalisation des événements

CloudTrail est automatiquement activé sur votre ordinateur Compte AWS et enregistre les événements en cas d'activité. Les ressources suivantes peuvent vous aider à en savoir plus sur la journalisation et le suivi des événements de connexion.

- CloudTrail enregistre les tentatives de connexion au AWS Management Console. Tous les événements de connexion des utilisateurs IAM, des utilisateurs root et des utilisateurs fédérés génèrent des enregistrements dans CloudTrail des fichiers journaux. Pour plus d'informations, veuillez consulter la rubrique Événements de connexion AWS Management Console dans le Guide de l'utilisateur AWS CloudTrail .
- Si vous utilisez un point de terminaison régional pour vous connecter au AWS Management Console, CloudTrail enregistre l'`ConsoleLogin`événement dans la région appropriée pour le point de terminaison. Pour plus d'informations sur les AWS Sign-In points de terminaison, consultez la section AWS Sign-In Points de terminaison et quotas dans le Guide de référence AWS général.
- Pour en savoir plus sur la façon dont CloudTrail les événements de connexion sont enregistrés pour IAM Identity Center, consultez la section Comprendre les événements de connexion d'IAM Identity Center dans le guide de l'utilisateur d'IAM Identity Center.
- Pour en savoir plus sur la façon dont CloudTrail les différentes informations d'identité utilisateur sont enregistrées dans IAM, consultez la section Journalisation des appels IAM et AWS STS API AWS CloudTrail dans le guide de l'Gestion des identités et des accès AWS utilisateur.

AWS Sign-In prend en charge les politiques basées sur les ressources et les politiques de contrôle des ressources qui vous permettent de restreindre l'accès à la console en fonction de l'emplacement du réseau et de l'identité principale. Pour les utilisateurs root, l'emplacement réseau est validé avant que l'invite de mot de passe ne s'affiche. Pour tous les types principaux, les politiques sont évaluées avant et après l'authentification. Pour de plus amples informations, veuillez consulter Contrôle de l'accès à la console à l'aide de politiques basées sur les ressources et de politiques de contrôle des ressources.

Déterminez votre type d'utilisateur

La façon dont vous vous connectez dépend du type d' AWS utilisateur que vous êtes. Vous pouvez gérer un Compte AWS utilisateur root, un utilisateur IAM, un utilisateur dans IAM Identity Center ou une identité fédérée. Vous pouvez utiliser un profil AWS Builder ID pour accéder à certains AWS services et outils. Les différents types d'utilisateurs sont répertoriés ci-dessous.

Rubriques

Utilisateur root

Également appelé propriétaire du compte ou utilisateur root du compte. En tant qu'utilisateur root, vous avez un accès complet à tous les AWS services et ressources de votre Compte AWS. Lorsque vous créez un Compte AWS, vous commencez par une identité de connexion unique offrant un accès complet à tous les AWS services et ressources du compte. Cette identité est celle de l'utilisateur root du AWS compte. Vous pouvez vous connecter en tant qu'utilisateur racine avec l'adresse e-mail et le mot de passe que vous avez utilisés pour créer le compte. Les utilisateurs root se connectent à l'aide du AWS Management Console. Pour obtenir des instructions détaillées sur la procédure de connexion, consultezConnectez-vous en AWS Management Console tant qu'utilisateur root.

> **Important**
>
> 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.

Pour plus d'informations sur les identités IAM, y compris l'utilisateur root, consultez Identités IAM (utilisateurs, groupes d'utilisateurs et rôles).

Utilisateur IAM

Un utilisateur IAM est une entité dans AWS laquelle vous créez. Cet utilisateur est une identité au sein de vous Compte AWS qui a obtenu des autorisations personnalisées spécifiques. Vos informations d'identification d'utilisateur IAM se composent d'un nom et d'un mot de passe utilisés pour vous connecter au AWS Management Console. Pour obtenir des instructions détaillées sur la procédure de connexion, consultezConnectez-vous au en AWS Management Console tant qu'utilisateur IAM.

Pour plus d'informations sur les identités IAM, y compris l'utilisateur IAM, consultez Identités IAM (utilisateurs, groupes d'utilisateurs et rôles).

Utilisateur du centre d'identité IAM

Un utilisateur de l'IAM Identity Center est membre de plusieurs applications AWS Organizations Comptes AWS et peut y accéder par le biais de votre portail AWS d'accès. Si leur entreprise a intégré Active Directory ou un autre fournisseur d'identité à IAM Identity Center, les utilisateurs d'IAM Identity Center peuvent utiliser leurs informations d'identification d'entreprise pour se connecter. IAM Identity Center peut également être un fournisseur d'identité permettant à un administrateur de créer des utilisateurs. Quel que soit le fournisseur d'identité, les utilisateurs d'IAM Identity Center se connectent à l'aide de votre portail d' AWS accès, qui est une URL de connexion spécifique à leur organisation. Les utilisateurs d'IAM Identity Center ne peuvent pas se connecter via l' AWS Management Console URL.

Les utilisateurs humains d'IAM Identity Center peuvent obtenir l'URL de votre portail AWS d'accès de l'une des manières suivantes :

- Un message de leur administrateur ou d'un employé du service d'assistance
- Un e-mail AWS contenant une invitation à rejoindre IAM Identity Center

> **Tip**
>
> Tous les e-mails envoyés par le service IAM Identity Center proviennent de l'adresse no-reply@signin.aws ou no-reply@login.awsapps.com. Nous vous recommandons de configurer

votre système de messagerie de manière à ce qu'il accepte les e-mails provenant de ces adresses d'expéditeur et qu'il ne les traite pas comme du courrier indésirable ou du spam.

Pour obtenir des instructions détaillées sur la procédure de connexion, consultezConnectez-vous à votre AWS portail d'accès.

> **Note**
>
> Nous vous recommandons d'ajouter à vos favoris l'URL de connexion spécifique à votre organisation pour votre portail AWS d'accès afin de pouvoir y accéder ultérieurement.

Pour plus d'informations sur IAM Identity Center, voir Qu'est-ce qu'IAM Identity Center ?

Identité fédérée

Une identité fédérée est un utilisateur qui peut se connecter à l'aide d'un fournisseur d'identité externe (IdP) connu, tel que Login with Amazon, Facebook, Google ou tout autre IdP compatible avec OpenID Connect (OIDC). Avec la fédération des identités Web, vous pouvez recevoir un jeton d'authentification, puis échanger ce jeton contre des informations d'identification de sécurité temporaires associées à un rôle IAM autorisé à utiliser les ressources de votre Compte AWS. AWS Vous ne vous connectez pas avec le portail AWS Management Console ou n' AWS y accédez pas. C'est plutôt l'identité externe utilisée qui détermine la façon dont vous vous connectez.

Pour de plus amples informations, veuillez consulter Connectez-vous en tant qu'identité fédérée.

AWS Utilisateur Builder ID

En tant qu'utilisateur AWS Builder ID, vous vous connectez spécifiquement au AWS service ou à l'outil auquel vous souhaitez accéder. Un utilisateur AWS Builder ID complète ceux Compte AWS que vous possédez déjà ou que vous souhaitez créer. Un AWS Builder ID vous représente en tant que personne, et vous pouvez l'utiliser pour accéder à AWS des services et à des outils sans Compte AWS. Vous avez également un profil dans lequel vous pouvez consulter et mettre à jour vos informations. Pour de plus amples informations, veuillez consulter Connectez-vous avec ID de constructeur AWS.

AWS Le Builder ID est distinct de votre abonnement à AWS Skill Builder, un centre de formation en ligne où vous pouvez apprendre auprès d' AWS experts et développer des compétences en matière de cloud en ligne. Pour plus d'informations sur AWS Skill Builder, consultez AWS Skill Builder.

Déterminez votre URL de connexion

Utilisez l'une des URL suivantes pour y accéder AWS en fonction du type d' AWS utilisateur que vous êtes. Pour de plus amples informations, veuillez consulter Déterminez votre type d'utilisateur.

Rubriques

Compte AWS URL de connexion de l'utilisateur root

L'utilisateur root y accède AWS Management Console depuis la page de AWS connexion :. `https://console.aws.amazon.com/`

Cette page de connexion permet également de se connecter en tant qu'utilisateur IAM.

AWS portail d'accès

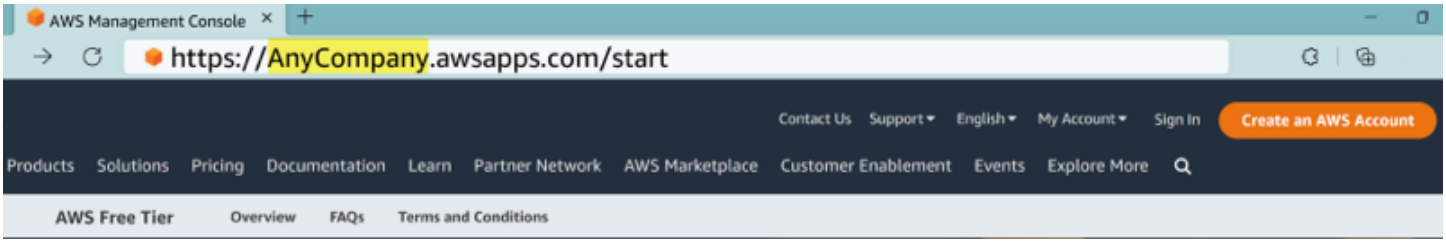
Le portail AWS d'accès est une URL de connexion spécifique permettant aux utilisateurs d'IAM Identity Center de se connecter et d'accéder à votre compte. Lorsqu'un administrateur crée l'utilisateur dans IAM Identity Center, il choisit si l'utilisateur reçoit soit une invitation par e-mail à rejoindre IAM Identity Center, soit un message de l'administrateur ou d'un employé du service d'assistance contenant un mot de passe à usage unique et l'URL du portail AWS d'accès. Le format d'une URL de connexion spécifique est similaire aux exemples suivants :

```
https://d-xxxxxxxxxx.awsapps.com/start
```

or

```
https://your_subdomain.awsapps.com/start
```

L'URL de connexion spécifique varie car votre administrateur peut la personnaliser. L'URL de connexion spécifique peut commencer par la lettre D suivie de 10 chiffres et lettres aléatoires. Votre sous-domaine peut également être utilisé dans l'URL de connexion et peut inclure le nom de votre entreprise, comme dans l'exemple suivant :



> **Note**
>
> Nous vous recommandons de mettre en signet l'URL de connexion spécifique à votre portail AWS d'accès afin de pouvoir y accéder ultérieurement.

Pour plus d'informations sur votre portail AWS d'accès, consultez la section Utilisation du portail AWS d'accès.

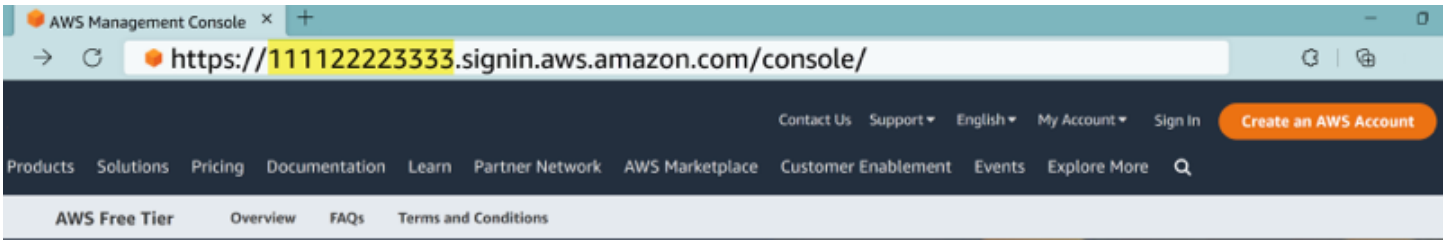
URL de connexion de l'utilisateur IAM

Les utilisateurs IAM peuvent y accéder à l' AWS Management Console aide d'une URL de connexion utilisateur IAM spécifique. L'URL de connexion de l'utilisateur IAM combine votre Compte AWS identifiant ou alias et `signin.aws.amazon.com/console`

Voici un exemple de ce à quoi ressemble l'URL de connexion d'un utilisateur IAM :

```
https://account_alias_or_id.signin.aws.amazon.com/console/
```

Si votre identifiant de compte est 111122223333, votre URL de connexion sera :



Si vous rencontrez des problèmes pour accéder Compte AWS à votre URL de connexion utilisateur IAM, consultez Resilience in Gestion des identités et des accès AWS pour plus d'informations.

URL d'identité fédérée

L'URL de connexion pour une identité fédérée varie. L'identité externe ou le fournisseur d'identité externe (IdP) détermine l'URL de connexion pour les identités fédérées. L'identité externe peut être Windows Active Directory, Login with Amazon, Facebook ou Google. Contactez votre administrateur pour plus de détails sur la procédure de connexion en tant qu'identité fédérée.

Pour plus d'informations sur les identités fédérées, consultez À propos de la fédération des identités Web.

AWS URL de l'identifiant du constructeur

L'URL de votre profil AWS Builder ID esthttps://profile.aws.amazon.com/. Lorsque vous utilisez votre identifiant AWS Builder, l'URL de connexion dépend du service auquel vous souhaitez accéder. Par exemple, pour vous connecter à Amazon CodeCatalyst, rendez-vous surhttps://codecatalyst.aws/login.

Domaines à ajouter à votre liste d'autorisations

Si vous filtrez l'accès à des AWS domaines ou points de terminaison d'URL spécifiques à l'aide d'une solution de filtrage de contenu Web telle que les pare-feux de nouvelle génération (NGFW) ou les passerelles Web sécurisées (SWG), vous devez ajouter les domaines ou points de terminaison d'URL suivants aux listes d'autorisation de votre solution de filtrage de contenu Web.

AWS Sign-In domaines à autoriser

Si vous ou votre organisation implémentez le filtrage des adresses IP ou des domaines, vous devrez peut-être autoriser les domaines de la liste à utiliser le AWS Management Console. Les domaines suivants doivent être accessibles sur le réseau à partir duquel vous essayez d'accéder au AWS Management Console.

- *[Region]*.signin.aws
- *[Region]*.signin.aws.amazon.com
- signin.aws.amazon.com
- *.cloudfront.net
- opfcaptcha-prod.s3.amazonaws.com

AWS Sign-In domaines d'administration à autoriser

Si vous configurez les contrôles d'accès à la console à l'aide de la AWS CLI, vous devez autoriser la liste des points de terminaison du plan AWS Sign-In de contrôle. Ce point de terminaison gère l'administration des politiques et est distinct des domaines de connexion à la console décrits dans la section précédente.

- `signin.[Region].api.aws`

  Remplacez *[Region]* par la AWS région que vous appelez. Disponible dans toutes les régions commerciales. Exemple: `signin.us-east-1.api.aws`.

Portail d'accès AWS domaines à autoriser

Si vous filtrez l'accès à des AWS domaines ou points de terminaison d'URL spécifiques à l'aide d'une solution de filtrage de contenu Web telle que les pare-feux de nouvelle génération (NGFW) ou les passerelles Web sécurisées (SWG), vous devez ajouter les domaines ou points de terminaison d'URL suivants aux listes d'autorisation de votre solution de filtrage de contenu Web. Cela vous permet d'accéder à votre Portail d'accès AWS.

Les listes suivantes indiquent les domaines IPv4 et à double pile ainsi que les points de terminaison d'URL à ajouter aux listes d'autorisation de votre solution de filtrage de contenu Web. Pour plus d'informations sur les points de terminaison à double pile, voir Mettre à jour les pare-feux et les passerelles pour autoriser l'accès à ceux-ci Portail d'accès AWS dans le guide de l'utilisateur d'IAM Identity Center.

Liste des autorisations IPv4

- *[Directory ID or alias]*`.awsapps.com`
- *[IAM Identity Center instance ID]*`.`*[Region]*`.portal.amazonaws.com`
- `*.aws.dev`
- `*.awsstatic.com`
- `*.console.aws.a2z.com`
- `oidc.`*[Region]*`.amazonaws.com`
- `*.sso.amazonaws.com`
- `*.sso.`*[Region]*`.amazonaws.com`

- *.sso-portal.*[Region]*.amazonaws.com

Dual-stack liste d'autorisations

- *[IAM Identity Center instance ID]*.portal.*[Region]*.app.aws
- *.aws.dev
- *.awsstatic.com
- *.console.aws.a2z.com
- oidc.*[Region]*.api.aws
- sso.*[Region]*.api.aws
- portal.sso.*[Region]*.api.aws
- *[Region]*.sso.signin.aws
- *[Region]*.signin.aws.amazon.com
- signin.aws.amazon.com
- *.cloudfront.net
- cdn.us-east-1.threat-mitigation.aws.amazon.com
- us-east-1.threat-mitigation.aws.amazon.com
- amcs-captcha-prod-us-east-1.s3.dualstack.us-east-1.amazonaws.com

ID de constructeur AWS domaines à autoriser

Si vous ou votre organisation implémentez le filtrage des adresses IP ou des domaines, vous devrez peut-être autoriser les domaines à créer et à utiliser un ID de constructeur AWS. Les domaines suivants doivent être accessibles sur le réseau à partir duquel vous essayez d'accéder ID de constructeur AWS.

- view.awsapps.com/start
- *.portal.*.app.aws
- *.aws.dev
- *.api.aws
- *.uis.awsstatic.com
- *.console.aws.a2z.com
- oidc.*.amazonaws.com

- `oidc.*.api.aws`
- `*.sso.amazonaws.com`
- `*.sso.*.amazonaws.com`
- `*.sso-portal.*.amazonaws.com`
- `sso.*.api.aws`
- `*.signin.aws`
- `*.cloudfront.net`
- `opfcaptcha-prod.s3.amazonaws.com`
- `profile.aws.amazon.com`

Bonnes pratiques en matière de sécurité pour Compte AWS administrateurs

Si vous êtes un administrateur de compte qui en a créé un nouveau Compte AWS, nous recommandons de suivre les étapes suivantes pour aider vos utilisateurs à suivre les meilleures pratiques de AWS sécurité lorsqu'ils se connectent.

1. Connectez-vous en tant qu'utilisateur root pour activer l'authentification multifactorielle (MFA) et créez AWS un utilisateur administratif dans IAM Identity Center si ce n'est déjà fait. Ensuite, protégez vos informations d'identification root et ne les utilisez pas pour les tâches quotidiennes.
2. Connectez-vous en tant qu' Compte AWS administrateur et configurez les identités suivantes :
   - Créez des utilisateurs ayant le moins de privilèges pour d'autres humains.
   - Configurez des informations d'identification temporaires pour les charges de travail.
   - Créez des clés d'accès uniquement pour les cas d'utilisation nécessitant des informations d'identification à long terme.
3. Ajoutez des autorisations pour autoriser l'accès à ces identités. Vous pouvez commencer par les politiques AWS gérées et passer aux autorisations du moindre privilège.
   - Ajoutez des ensembles d'autorisations aux utilisateurs d' AWS IAM Identity Center (successeur de AWS Single Sign-On).
   - Ajoutez des politiques basées sur l'identité aux rôles IAM utilisés pour les charges de travail.
   - Ajoutez des politiques basées sur l'identité pour les utilisateurs IAM pour les cas d'utilisation nécessitant des informations d'identification à long terme.

- Pour plus d'informations sur les utilisateurs IAM, consultez la section Bonnes pratiques en matière de sécurité dans IAM.

4. Enregistrez et partagez des informations surConnectez-vous au AWS Management Console. Ces informations varient en fonction du type d'identité que vous avez créé.
5. Tenez à jour l'adresse e-mail de votre utilisateur root et le numéro de téléphone du contact principal de votre compte afin de pouvoir recevoir les notifications importantes relatives au compte et à la sécurité.

   - Modifiez le nom du compte, l'adresse e-mail ou le mot de passe du Utilisateur racine d'un compte AWS.
   - Accédez au contact principal du compte ou mettez-le à jour.
6. Consultez les meilleures pratiques de sécurité dans IAM pour en savoir plus sur les meilleures pratiques supplémentaires en matière de gestion des identités et des accès.
7. Mettez en œuvre des contrôles d'accès basés sur le réseau : utilisez des politiques Sign-in basées sur les ressources ou des politiques de contrôle des ressources (RCP) pour limiter la connexion à la console aux demandes provenant de plages d'adresses IP ou de VPC approuvés. Pour les environnements utilisant l'accès privé à la console, configurez les politiques de point de terminaison VPC pour contrôler les comptes accessibles via vos points de terminaison (voir Accès privé à la console). Ensemble, les politiques Sign-in basées sur les ressources, les RCP et les politiques de point de terminaison VPC fournissent des contrôles réseau en couches à différents points d'application. Pour les utilisateurs root, les Sign-in politiques bloquent entièrement la page d'identification en cas de tentative d'accès depuis des réseaux non autorisés. AWS recommande de configurer les principaux exclus pour l'accès de restauration afin d'éviter le verrouillage du compte, bien que cela soit facultatif. Pour de plus amples informations, veuillez consulter Contrôle de l'accès à la console à l'aide de politiques basées sur les ressources et de politiques de contrôle des ressources.

Connectez-vous au AWS Management Console

Lorsque vous vous connectez à AWS Management Console partir de l'URL de AWS connexion principale (https://console.aws.amazon.com/), vous devez choisir votre type d'utilisateur, utilisateur root ou utilisateur IAM. Si vous ne savez pas quel type d'utilisateur vous êtes, consultezDéterminez votre type d'utilisateur.

L'utilisateur root dispose d'un accès illimité au compte et est associé à la personne qui a créé le Compte AWS. L'utilisateur root crée ensuite d'autres types d'utilisateurs, tels que les utilisateurs IAM et utilisateurs dans AWS IAM Identity Center leur attribue des informations d'accès.

Un utilisateur IAM est une identité au sein de vous Compte AWS qui possède des autorisations personnalisées spécifiques. Lorsqu'un utilisateur IAM se connecte, il peut utiliser une URL de connexion qui inclut son alias Compte AWS ou son alias, par exemple à la `https://account_alias_or_id.signin.aws.amazon.com/console/` place de l'URL de AWS connexion principale. `https://console.aws.amazon.com/`

Vous pouvez vous connecter à un maximum de 5 identités différentes simultanément dans un seul navigateur dans le AWS Management Console. Il peut s'agir d'une combinaison d'utilisateurs root, d'utilisateurs IAM ou de rôles fédérés dans différents comptes ou dans le même compte. Pour plus de détails, consultez la section Connexion à plusieurs comptes dans le Guide de démarrage AWS Management Console .

Tutoriels

- Connectez-vous en AWS Management Console tant qu'utilisateur root
- Connectez-vous au en AWS Management Console tant qu'utilisateur IAM

Si vous ne savez pas quel type d'utilisateur vous êtes, consultezDéterminez votre type d'utilisateur.

Tutoriels

- Connectez-vous en AWS Management Console tant qu'utilisateur root
- Connectez-vous au en AWS Management Console tant qu'utilisateur IAM

Connectez-vous en AWS Management Console tant qu'utilisateur root

Lorsque vous créez un Compte AWS, vous commencez par une identité de connexion unique qui donne un accès complet à toutes Services AWS les ressources du compte. Cette identité est appelée utilisateur Compte AWS root et est accessible en vous connectant avec l'adresse e-mail et le mot de passe que vous avez utilisés pour créer le compte.

> **Important**
>
> Il est vivement recommandé de ne pas utiliser l'utilisateur racine pour vos tâches quotidiennes. Protégez vos informations d'identification d'utilisateur racine et utilisez-les pour effectuer les tâches que seul l'utilisateur racine peut effectuer. Pour obtenir la liste complète des tâches qui vous imposent de vous connecter en tant qu'utilisateur racine, consultez Tâches nécessitant des informations d'identification d'utilisateur racine dans le Guide de l'utilisateur IAM.

Pour vous connecter en tant qu'utilisateur root

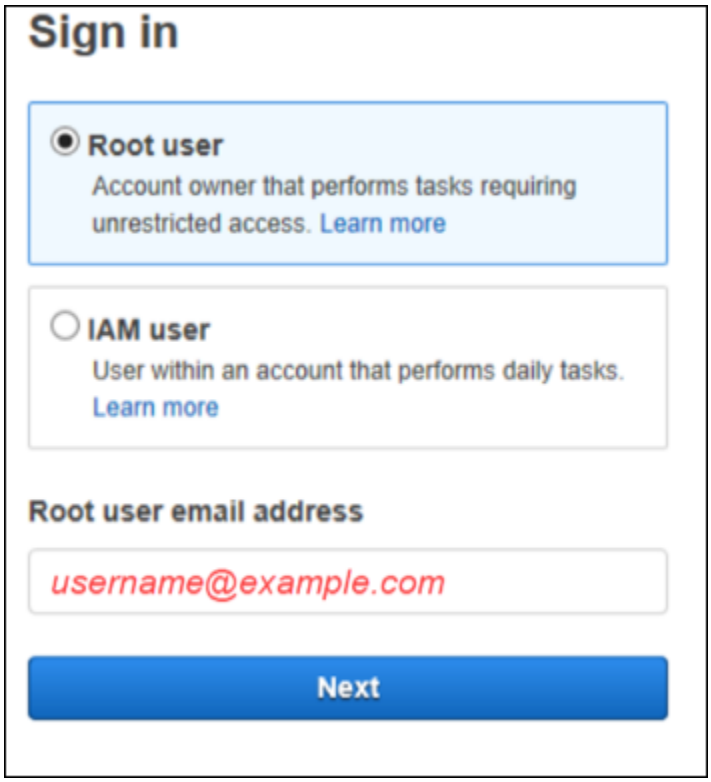
Vous pouvez vous connecter en tant qu'utilisateur root alors que vous êtes déjà connecté sous une autre identité dans le AWS Management Console. Pour plus de détails, consultez la section Connexion à plusieurs comptes dans le Guide de démarrage AWS Management Console .

Comptes AWS managed using ne AWS Organizations possède peut-être pas les informations d'identification de l'utilisateur root, et vous devez contacter un administrateur pour effectuer des actions d'utilisateur root sur votre compte membre. Si vous ne parvenez pas à vous connecter en tant qu'utilisateur root, consultezRésolution des problèmes Compte AWS problèmes de connexion.

1. Ouvrez le AWS Management Console chathttps://console.aws.amazon.com/.

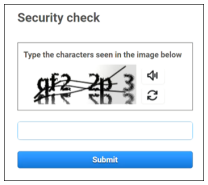
   > **Note**
   >
   > Si vous vous êtes déjà connecté en tant qu'utilisateur IAM à l'aide de ce navigateur, celui-ci peut afficher la page de connexion de l'utilisateur IAM à la place. Choisissez Se connecter en utilisant l'adresse e-mail de l'utilisateur root.

2. Choisissez l'utilisateur root.



3. Sous Adresse e-mail de l'utilisateur root, entrez l'adresse e-mail associée à votre utilisateur root. Sélectionnez ensuite Next.
4. Si vous êtes invité à effectuer un contrôle de sécurité, entrez les caractères qui vous sont présentés pour continuer. Si vous ne parvenez pas à terminer le contrôle de sécurité, essayez d'écouter le son ou d'actualiser le contrôle de sécurité pour y ajouter un nouveau jeu de caractères.

> **Tip**
>
> Tapez les caractères alphanumériques que vous voyez (ou entendez) dans l'ordre, sans espaces.



5. Entrez votre mot de passe.

6. Authentifiez-vous avec le MFA. La MFA est appliquée par défaut à l'utilisateur root. Pour les utilisateurs root de comptes autonomes et de comptes membres, vous devez activer manuellement le MFA, ce qui est fortement recommandé. Pour plus d'informations, consultez la section Authentification multifactorielle pour l'utilisateur Compte AWS root dans le guide de Gestion des identités et des accès AWS l'utilisateur.

   > **Tip**
   >
   > Pour des raisons de sécurité, nous vous recommandons de supprimer toutes les informations d'identification des utilisateurs root des comptes membres de votre AWS organisation afin d'empêcher toute utilisation non autorisée. Si vous choisissez cette option, les comptes membres ne peuvent pas se connecter en tant qu'utilisateur root, récupérer le mot de passe ou configurer le MFA. Dans ce cas, seul l'administrateur du compte de gestion peut effectuer une tâche qui nécessite les informations d'identification de l'utilisateur root dans un compte membre. Pour plus de détails, voir Gestion centralisée de l'accès root pour les comptes des membres dans le Guide de Gestion des identités et des accès AWS l'utilisateur.

7. Choisissez Sign in (Connexion). Le AWS Management Console apparaît.

Après authentification, la page d'accueil de la console AWS Management Console s'ouvre.

Informations supplémentaires

Pour plus d'informations sur l'utilisateur Compte AWS root, consultez les ressources suivantes.

- Pour un aperçu de l'utilisateur root, voir utilisateur Compte AWS root.
- Pour plus de détails sur l'utilisation de l'utilisateur root, consultez la section Utilisation de l'utilisateur Compte AWS root.
- Pour step-by-step savoir comment réinitialiser le mot de passe de votre utilisateur root, consultezJ'ai oublié le mot de passe de mon utilisateur root pour mon Compte AWS.

Connectez-vous au en AWS Management Console tant qu'utilisateur IAM

Un utilisateur IAM est une identité créée au sein d'un Compte AWS utilisateur autorisé à interagir avec les AWS ressources. Les utilisateurs IAM se connectent à l'aide de leur identifiant de compte ou alias, de leur nom d'utilisateur et d'un mot de passe. Les noms d'utilisateur IAM sont configurés par votre administrateur. Les noms d'utilisateur IAM peuvent être soit des noms conviviaux*Zhang*, soit des adresses e-mail telles que*zhang@example.com*. Les noms d'utilisateur IAM ne peuvent pas inclure d'espaces, mais peuvent inclure des lettres majuscules et minuscules, des chiffres et des symboles`+ = , . @ _ -`.

> **Tip**
>
> Si l'authentification multifactorielle (MFA) est activée pour votre utilisateur IAM, vous devez avoir accès au dispositif d'authentification. Pour plus de détails, consultez la section Utilisation d'appareils MFA avec votre page de connexion IAM.

Pour vous connecter en tant qu'utilisateur IAM

Vous pouvez vous connecter en tant qu'utilisateur IAM alors que vous êtes déjà connecté sous une autre identité dans le AWS Management Console. Pour plus de détails, consultez la section Connexion à plusieurs comptes dans le Guide de démarrage AWS Management Console .

1. Ouvrez le AWS Management Console chathttps://console.aws.amazon.com/.
2. La page de connexion principale apparaît. Entrez l'identifiant du compte (12 chiffres) ou l'alias, votre nom d'utilisateur IAM et votre mot de passe.

> **Note**
>
> Il se peut que vous n'ayez pas à saisir votre identifiant de compte ou votre alias si vous vous êtes déjà connecté en tant qu'utilisateur IAM avec votre navigateur actuel ou si vous utilisez l'URL de connexion de votre compte.

3. Choisissez Sign in (Connexion).
4. Si le MFA est activé pour votre utilisateur IAM, vous devez confirmer votre identité à l'aide d' AWS un authentificateur. Pour plus d'informations, consultez la section Utilisation de l'authentification multifactorielle (MFA) dans. AWS

Après authentification, la page d'accueil de la console AWS Management Console s'ouvre.

Informations supplémentaires

Pour plus d'informations sur les utilisateurs IAM, consultez les ressources suivantes.

- Pour une présentation de l'IAM, voir What is Identity and Access Management ?
- Pour en savoir plus sur IDs le AWS compte, consultez l'ID de votre AWS compte et son alias.
- Pour step-by-step savoir comment réinitialiser votre mot de passe utilisateur IAM, consultezJ'ai oublié mon mot de passe utilisateur IAM pour mon Compte AWS.

Contrôle de l'accès à la console à l'aide de politiques basées sur les ressources et de politiques de contrôle des ressources

> **Important**
>
> L'accès à la connexion à la console est activé par défaut. AWS Sign-In autorise initialement un accès illimité à la console. Pour ajouter des restrictions, activez la configuration des autorisations de console pour votre compte ou votre organisation. Les déclarations d'autorisation des ressources que vous créez n'ont aucun effet tant que vous n'activez pas l'autorisation de la console. Consultez Commencer à contrôler l'accès à la console à l'aide de politiques de ressources.

AWS Sign-In prend en charge les politiques basées sur les ressources et les politiques de contrôle des ressources (RCP) pour contrôler l'accès à. AWS Sign-In Utilisez ces politiques pour vérifier l'identité de l'utilisateur et l'emplacement du réseau tout au long de l' AWS Management Console accès, avant, pendant et après l'authentification. Pour les utilisateurs root, ces politiques valident l'emplacement du réseau et l'identité de l'utilisateur avant le début de la collecte des informations d'identification. Les informations d'identification ne peuvent être saisies que lorsque l'accès provient des réseaux attendus.

AWS Sign-In politiques basées sur les ressources :

- S'applique à des AWS comptes individuels.
- Permettez aux administrateurs de compte de restreindre l'accès à la console en fonction des paramètres réseau et des principales identités.

Politiques de contrôle des ressources (RCP) :

- Appliquez à l'échelle de l'organisation via AWS Organizations.
- Fournissez une gouvernance centralisée pour tous les comptes des membres.

Les deux types de politique vérifient l'accès avant l'authentification. Cela empêche les principaux d'accéder à la page de connexion depuis des réseaux inattendus.

Ces politiques ne remplacent pas les politiques basées sur l'identité IAM, qui continuent de s'appliquer.

> **Note**
>
> Pour une documentation complète sur les politiques de contrôle des ressources, y compris la configuration et la gestion au niveau de l'organisation, consultez les politiques de contrôle des ressources dans le guide de l'utilisateur d'AWS Organizations. Cette section se concentre principalement sur les politiques AWS Sign-In basées sur les ressources.

AWS Sign-In les politiques basées sur les ressources et les RCP s'appliquent aux méthodes d'authentification suivantes :

- AWS Management Console— Connexion directe à l'aide de la page de connexion de la console.
- AWS IAM Identity Center : connexion à la console à l'aide d'IAM Identity Center.
- Fournisseurs d'identité fédérés : Sign-in via la fédération SAML ou OIDC.
- Applications intégrées à AWS Sign-In : Amazon Connect, Amazon QuickSight, AWS Health Dashboard, Amazon AppStream, Amazon Lightsail, AWS IQ.

Ces contrôles ne s'appliquent pas à l'accès programmatique à l'aide de clés d'accès (AWS SDK ou appels d'API signés avec SigV4).

Comment ? AWS Sign-In évalue les politiques basées sur les ressources

AWS Sign-In évalue les politiques basées sur les ressources ou les politiques de contrôle des ressources (RCP) applicables à deux moments lors de l'accès à la console : avant l'authentification (phase de pré-authentification) et après authentification réussie (phase de post-authentification). Chaque évaluation vérifie les clés de condition définies dans votre politique. Les touches disponibles dépendent de la phase et de l'action. Pour en savoir plus, consultez Clés de condition prises en charge.

> **Note**
>
> Pour la connexion de l'utilisateur root, toute tentative d'accès à partir de réseaux inattendus est bloquée avant que l'invite de mot de passe ne s'affiche. Cela empêche la soumission d'informations d'identification provenant de réseaux inattendus.

Après l'authentification, l'évaluation prend également en compte les politiques basées sur l'identité du principal. Une politique IAM qui refuse l'action de connexion appropriée peut empêcher l'octroi de la session de console, même lorsque les conditions du réseau sont remplies.

Actions prises en charge

AWS Sign-In les politiques relatives aux ressources (politiques basées sur les ressources et RCP) soutiennent les actions suivantes :

`signin:Authenticate`

Il s'agit d'une action d'évaluation uniquement (non appelable) qui est évaluée lorsqu'une demande de connexion est reçue. Il s'agit d'une vérification préalable à l'authentification qui se produit lorsque le principal saisit les informations d'identification sur la page de connexion (utilisateur root, utilisateur IAM) ou initie la connexion à la console à l'aide des informations d'identification d'un fournisseur d'identité ou d'AWS STS (utilisateur fédéré, rôle).

Clés de condition prises en charge : `aws:SourceIpaws:SourceVpc,aws:SourceVpce,aws:VpcSourceIp,aws:RequestedRegion,,si`

Principal-based les clés de condition globales (`aws:PrincipalArn,aws:PrincipalAccount`) ne sont pas disponibles pour cette action car l'identité de l'utilisateur n'a pas encore été confirmée.

`signin:AuthorizeOAuth2Access`

Utilisé pour la génération de code d'autorisation OAuth. Une fois l'authentification réussie, cette action est déclenchée lorsque le système génère un code d'autorisation OAuth. À ce stade, l'utilisateur est authentifié et les clés de condition basées sur le principal sont disponibles.

Clés de condition prises en charge : `aws:SourceIpaws:SourceVpc,aws:SourceVpce,aws:VpcSourceIp,aws:RequestedRegion,aws`

`signin:CreateOAuth2Token`

Cette action de post-authentification est utilisée pour la création et l'échange de jetons OAuth. Cette action est déclenchée lors de l'échange de codes d'autorisation contre des jetons d'accès, de l'actualisation des jetons ou de l'exécution d'opérations d'échange de jetons. Principal-based les clés de condition sont disponibles pendant cette phase.

Clés de condition prises en charge : `aws:SourceIpaws:SourceVpc`,`aws:SourceVpce`,`aws:VpcSourceIp`,`aws:RequestedRegion`,`aws`

> **Important**
>
> Lorsque vous créez des AWS Sign-In politiques (politiques basées sur les ressources ou RCP), couvrez les trois actions de votre politique : `signin:Authenticate` dans une déclaration de pré-authentification `signin:AuthorizeOAuth2Access` et `signin:CreateOAuth2Token` dans une déclaration de post-authentification. La connexion à la console utilise OAuth 2.0, qui exécute les trois actions de manière séquentielle. Si votre politique omet une action, la phase correspondante n'est pas protégée. Pour les actions de politique relatives aux points de terminaison VPC`signin:CreateAccount`, notamment, consultez AWS Management Console Private Access.

Clés de condition prises en charge

AWS Sign-In prend en charge les clés de condition suivantes dans les politiques basées sur les ressources et les politiques de contrôle des ressources (RCP). Utilisez ces touches pour contrôler l'accès à la console en fonction de l'emplacement du réseau et de l'identité principale :

- Network-based (toutes les actions) :`aws:SourceIp`,`aws:SourceVpc`,`aws:SourceVpce`,`aws:VpcSourceIp`,`aws:RequestedReg`
- Identity-based (actions post-authentification) :`aws:PrincipalArn`,`aws:PrincipalAccount`.
- Service-specific (pré-authentification uniquement) :`signin:PrincipalArn`.

Pour les règles d'utilisation détaillées, la compatibilité des opérateurs, les restrictions de combinaison et la matrice de disponibilité par action, voirAWS Sign-In référence des clés de condition.

Commencer à contrôler l'accès à la console à l'aide de politiques de ressources

Conditions préalables

- AWS CLI installée et configurée.
- Autorisations IAM appropriées (voirAWS politique gérée : AWSSignInResourcePolicyManagement).
- Périmètres réseau identifiés (plages d'adresses IP, VPC ou points de terminaison VPC).
- Principaux exclus désignés pour conserver l'accès (recommandé mais facultatif).
- Si votre réseau utilise le filtrage des sorties, autorisez le point de terminaison du plan de AWS Sign-In contrôle sur la liste (voirAWS Sign-In domaines d'administration à autoriser).

> **Important**
>
> Avant d'activer l'autorisation de console en production, il est AWS recommandé de configurer au moins un principal exclu afin de conserver l'accès de restauration d'urgence. Tous les principaux, y compris l'utilisateur root, sont soumis à cette politique, sauf s'ils sont explicitement exclus. Les principaux exclus sont facultatifs, mais leur omission augmente le risque de verrouillage du compte en cas de modification inattendue des conditions du réseau.

Spécifiez toutes `--region us-east-1` les opérations d'écriture sur AWS Sign-In les politiques. AWS reproduit les politiques de cette région dans le monde entier. Les opérations de lecture peuvent cibler n'importe quelle région.

Étape 1 : créer des déclarations d'autorisation relatives aux ressources

Créez des déclarations d'autorisation qui définissent vos contrôles d'accès. Toutes les opérations d'écriture sont requises `--region us-east-1` (le AWS Sign-In service accepte les modifications de politique uniquement dans cette région). Les autres paramètres (`--source-vpc`,`--source-ip`,`--requested-region`,`--excluded-principal`) définissent les conditions de votre politique. Par exemple, `--requested-region us-west-2` ajoute une condition limitant la connexion au point de terminaison de connexion régional us-west-2.

Exemple — Restreindre l'accès au VPC d'entreprise :

```
aws signin put-resource-permission-statement \
  --source-vpc vpc-0abc123def456789 \
  --requested-region us-west-2 \
  --excluded-principal "arn:aws:iam::123456789012:user/EmergencyAdmin" \
  --client-token unique-request-id-12345 \
  --region us-east-1
```

Exemple — Restreindre l'accès à une plage d'adresses IP spécifique :

```
aws signin put-resource-permission-statement \
  --source-ip "IP_ADDRESS" \
  --excluded-principal "arn:aws:iam::123456789012:role/BreakGlassRole" \
  --region us-east-1
```

> **Note**
>
> Le `--excluded-principal` paramètre désigne un principal exclu qui contourne les restrictions du réseau, préservant ainsi l'accès d'urgence si les conditions du réseau changent.

Étape 2 : activer la configuration des autorisations de console

L'étape suivante active l'application des politiques pour le processus de connexion à la console sur votre compte ou votre organisation. Les déclarations d'autorisation des ressources peuvent être créées à tout moment, mais elles ne sont pas évaluées tant que l'autorisation de la console n'est pas activée.

> **Warning**
>
> L'activation de l'autorisation de console peut bloquer les principaux si les conditions de votre réseau sont mal configurées ou si une politique de contrôle des services (SCP) ou une politique de contrôle des ressources (RCP) existante refuse les actions. AWS Sign-In Avant d'activer l'autorisation de console, vérifiez que vos déclarations d'autorisation sont correctes et supprimez ou ajustez tout SCP ou RCP qui refuse `signin:Authenticatesignin:AuthorizeOAuth2Access`, ou. `signin:CreateOAuth2Token`

Pour les comptes autonomes :

```
aws signin put-console-authorization-configuration \
  --target-id <your-aws-account-id> \
  --region us-east-1
```

Pour les organisations AWS :

```
aws signin put-console-authorization-configuration \
  --target-id <your-aws-organization-id> \
  --region us-east-1
```

Vérifiez la configuration :

```
aws signin get-console-authorization-configuration \
  --target-id <your-target-id> \
  --region <your-region>
```

Supprimez la configuration d'autorisation de la console :

```
aws signin delete-console-authorization-configuration \
  --target-id <your-target-id> \
  --region us-east-1
```

Étape 3 : Vérifiez votre politique

Répertoriez toutes les déclarations d'autorisation :

```
aws signin list-resource-permission-statements \
  --max-results 50 \
  --region <your-region>
```

Récupérez la politique consolidée complète :

```
aws signin get-resource-policy \
  --region <your-region>
```

La `get-resource-policy` commande renvoie la politique complète basée sur les ressources composée de toutes vos déclarations d'autorisation. Passez en revue cette politique pour vous assurer qu'elle reflète les contrôles d'accès prévus avant de tester l'accès à la console.

Disponibilité par région

Les API d'autorisation de console sont disponibles dans toutes les régions AWS commerciales. Vous pouvez appeler ces API depuis n'importe quelle région dans laquelle vous opérez.

> **Important**
>
> Les opérations d'écriture (`put-console-authorization-configurationput-resource-permission-statement`,`delete-console-authorization-configuration`,,`delete-resource-permission-statement`) doivent être effectuées dans la `us-east-1` région. Les politiques créées dans `us-east-1` se répliquent automatiquement à l'échelle mondiale. Les opérations de lecture (`get-console-authorization-configuration`,`list-resource-permission-statements`,`get-resource-policy`) peuvent être effectuées depuis n'importe quelle région.

Comprendre la structure des politiques

AWS Sign-In les politiques contiennent deux instructions qui protègent les différentes phases du flux de connexion à la console :

- Pre-authentication déclaration (Action :**`signin:Authenticate`**) : évaluée lors de la réception de la demande de connexion, avant la fin de l'authentification. La clé globale n'`aws:PrincipalArn`est pas disponible à ce stade car l'identité du principal n'est pas confirmée. Au cours de cette phase, `signin:PrincipalArn` il est possible d'exempter des principaux spécifiques des restrictions du réseau. Network-based les clés de condition sont disponibles pour évaluation au cours de cette phase.
- Post-authentication statement (Action :**`signin:AuthorizeOAuth2Access`**,**`signin:CreateOAuth2Token`**) : évaluée après authentification, lors de l'échange de jetons OAuth. Utilisations `aws:PrincipalArn` pour exempter des principes spécifiques. Toutes les clés de condition basées sur le réseau et basées sur l'identité sont disponibles pour évaluation au cours de cette phase.

Les deux instructions sont obligatoires car la connexion à la console utilise OAuth 2.0, qui exécute les trois actions de manière séquentielle. Une politique comportant une seule déclaration laisse l'autre phase sans protection. `signin:PrincipalArn`prend en charge les types d'utilisateur root,

d'utilisateur IAM et de rôle principal. `aws:PrincipalArn`prend en charge tous les principaux types (utilisateur root, utilisateur IAM, utilisateur fédéré, rôle).

Exemples de politiques

Exemple 1 : RCP avec périmètre réseau et principaux exclus

La politique de contrôle des ressources (RCP) suivante interdit la AWS Management Console connexion depuis l'extérieur de votre réseau d'entreprise pour tous les comptes de votre organisation. Les principaux exclus désignés sont exemptés en cas d'accès d'urgence. Étant donné que les identifiants VPC ne sont uniques qu'au sein d'une région, la politique inclut une troisième instruction qui identifie l' VPC-based accès à la région attendue.

La `EnforceNetworkPerimeterPreAuth` déclaration est utilisée `signin:PrincipalArn` pour exempter les principaux exclus pendant la phase de pré-authentification. La `EnforceNetworkPerimeterPostAuth` déclaration est utilisée `aws:PrincipalArn` pour exempter les principaux exclus après authentification. L'`EnforceSourceVPCRegion`instruction garantit que la région de demande correspond à la région VPC, en limitant l'accès à la région attendue pour le VPC spécifié.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "EnforceNetworkPerimeterPreAuth",
      "Effect": "Deny",
      "Principal": "*",
      "Action": ["signin:Authenticate"],
      "Resource": "*",
      "Condition": {
        "ArnNotEquals": {
          "signin:PrincipalArn": [
            "arn:aws:iam::111122223333:root",
            "arn:aws:iam::444455556666:root",
            "arn:aws:iam::777788889999:user/EmergencyUser",
            "arn:aws:iam::777788889999:role/OrgBreakGlassRole"
          ]
        },
        "NotIpAddressIfExists": {
          "aws:SourceIp": "<my-corporate-cidr>"
        },
```

```
        "StringNotEquals": {
          "aws:SourceVpc": "<my-vpc>"
        }
      }
    },
    {
      "Sid": "EnforceNetworkPerimeterPostAuth",
      "Effect": "Deny",
      "Principal": "*",
      "Action": ["signin:CreateOAuth2Token", "signin:AuthorizeOAuth2Access"],
      "Resource": "*",
      "Condition": {
        "ArnNotEquals": {
          "aws:PrincipalArn": [
            "arn:aws:iam::111122223333:root",
            "arn:aws:iam::444455556666:root",
            "arn:aws:iam::777788889999:user/EmergencyUser",
            "arn:aws:iam::777788889999:role/OrgBreakGlassRole"
          ]
        },
        "NotIpAddressIfExists": {
          "aws:SourceIp": "<my-corporate-cidr>"
        },
        "StringNotEquals": {
          "aws:SourceVpc": "<my-vpc>"
        }
      }
    },
    {
      "Sid": "EnforceSourceVPCRegion",
      "Effect": "Deny",
      "Principal": "*",
      "Action": [
        "signin:Authenticate",
        "signin:CreateOAuth2Token",
        "signin:AuthorizeOAuth2Access"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:SourceVpc": "<my-vpc>"
        },
        "StringNotEqualsIfExists": {
          "aws:RequestedRegion": "<my-vpc-region>"
```

```
        }
      }
    }
  ]
}
```

Cette politique :

- Refuse l'accès à la page de connexion sauf si la demande provient de la plage d'adresses IP de l'entreprise ou du VPC de l'entreprise. Les comptes root et les utilisateurs IAM exclus sont exemptés via `signin:PrincipalArn` (pré-authentification).
- Refuse l'échange de jetons OAuth sauf s'il s'agit de la plage d'adresses IP de l'entreprise ou du VPC. Les comptes root, les utilisateurs IAM et les rôles exclus sont exemptés via `aws:PrincipalArn` (clé globale post-authentification).
- Si une demande provient du VPC spécifié mais que la région ne correspond pas, l'accès est refusé. AWS Les identifiants de VPC sont uniques au sein d'une région, et le même identifiant de VPC peut exister dans différentes régions.
- S'applique à l'ensemble de votre organisation AWS lorsqu'elle est configurée en tant que RCP.

Exemple 2 : Resource-based politique d' IP-based accès avec principal exclu

La politique basée sur les ressources suivante refuse l'accès à la console à tous les principaux effectuant des demandes en dehors de la plage d'adresses IP spécifiée, les principaux exclus étant exemptés. La politique contient deux instructions : une instruction de pré-authentification qui utilise la `signin:PrincipalArn` clé spécifique au service et une instruction de post-authentification qui utilise la clé globale. `aws:PrincipalArn`

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Principal": { "AWS": "*" },
      "Action": ["signin:Authenticate"],
      "Resource": "*",
      "Condition": {
        "ArnNotEquals": {
```

```
          "signin:PrincipalArn": "<excluded-principal-arn>"
        },
        "NotIpAddress": {
          "aws:SourceIp": "<my-corporate-cidr>"
        },
        "StringEquals": {
          "aws:ResourceAccount": "<my-aws-account-id>"
        }
      }
    },
    {
      "Effect": "Deny",
      "Principal": { "AWS": "*" },
      "Action": ["signin:CreateOAuth2Token", "signin:AuthorizeOAuth2Access"],
      "Resource": "*",
      "Condition": {
        "ArnNotEquals": {
          "aws:PrincipalArn": "<excluded-principal-arn>"
        },
        "NotIpAddress": {
          "aws:SourceIp": "<my-corporate-cidr>"
        },
        "StringEquals": {
          "aws:ResourceAccount": "<my-aws-account-id>"
        }
      }
    }
  ]
}
```

Cette politique :

- Refuse l'accès à tous les principaux sauf s'ils se connectent depuis la plage <my-corporate-cidr> d'adresses IP.
- Exempte le principal exclu des restrictions du réseau en utilisant `signin:PrincipalArn` (pré-authentification) et `aws:PrincipalArn` (post-authentification).
- S'applique uniquement au compte spécifique sur lequel la politique basée sur les ressources est configurée (identifié par<my-aws-account-id>).

Bonnes pratiques

Configurer les principaux exclus pour un accès de restauration d'urgence

AWS recommande de configurer au moins un utilisateur exclu avant d'appliquer les politiques d'autorisation de console en production. Au stade de la pré-authentification, la clé de `signin:PrincipalArn` condition exempte l'utilisateur root, l'utilisateur IAM et les principaux de rôle. Au stade de la post-authentification, la clé de `aws:PrincipalArn` condition exempte tous les types principaux (utilisateur root, utilisateur IAM, utilisateur fédéré, rôle).

Les principaux exclus sont facultatifs, mais leur omission augmente le risque de verrouillage du compte si les conditions du réseau changent de façon inattendue ou si les politiques sont mal configurées.

Étapes de configuration principales exclues recommandées :

1. Créez un rôle IAM exclu (par exemple,`BreakGlassRole`).
2. Pour les rôles exclus, exigez le MFA dans la politique de confiance des rôles.
3. Accordez à l'identité exclue uniquement les autorisations minimales nécessaires pour une restauration d'urgence.
4. Incluez l'ARN principal exclu dans les déclarations de politique de pré-authentification (`signin:PrincipalArn`) et de post-authentification (`aws:PrincipalArn`).
5. Documentez la procédure de récupération et stockez-la en toute sécurité à l'extérieur AWS.
6. Testez régulièrement l'accès principal exclu pour confirmer qu'il fonctionne en cas de besoin.

Gérez les chemins d'accès à la restauration

Outre le principal exclu décrit ci-dessus, assurez-vous que d'autres méthodes d'accès sont disponibles au cas où les politiques d'autorisation de la console bloqueraient la connexion de manière inattendue :

- Role-based accès par programmation : les politiques d'autorisation de la console s'appliquent uniquement à la connexion à la console interactive. Ils ne s'appliquent pas aux demandes d'API signées avec SigV4. Si vous disposez d'un accès programmatique (par exemple, des clés d'accès existantes, un rôle multicompte), utilisez-le pour appeler `signin:DeleteConsoleAuthorizationConfiguration` et supprimer la politique de restriction. Les informations d'identification doivent inclure

`signin:DeleteConsoleAuthorizationConfiguration` l'autorisation (incluse dans la politique `AWSSignInResourcePolicyManagement` gérée). AWS recommande des informations d'identification temporaires plutôt que des clés d'accès utilisateur IAM à long terme. Pour les comptes membres, les administrateurs des comptes de gestion peuvent `OrganizationAccountAccessRole` utiliser le compte membre (`aws sts assume-role`) pour obtenir ces informations d'identification temporaires.

- AWS rétablissement de l'assistance : maintenez à jour l'adresse e-mail et le numéro de téléphone de votre compte utilisateur root. Si l'accès principal exclu et l'accès programmatique ne sont pas disponibles, le AWS Support peut fournir un lien vers le portail de récupération après vérification de l'identité. Consultez L'accès à mon compte est bloqué après avoir activé l'autorisation de la console le processus de restauration complet.

Test avant le déploiement en production

AWS recommande de ne pas associer de RCP restrictifs à la racine de votre organisation sans avoir testé de manière approfondie l'impact de la politique sur les comptes. Créez plutôt une unité d'organisation dans laquelle vous pouvez déplacer vos comptes un par un, ou du moins en petit nombre, afin de ne pas empêcher les utilisateurs d'accéder à des comptes clés par inadvertance.

Flux de travail de test :

1. Créez une déclaration d'autorisation unique avec les restrictions de votre réseau principal.
2. Activez l'autorisation de console dans un compte hors production.
3. Testez l'accès à la console depuis les réseaux autorisés et refusés.
4. Consultez CloudTrail les journaux Amazon pour confirmer le comportement d'évaluation des politiques.
5. Testez l'accès à l'aide de votre principal exclu.
6. Étendez-vous progressivement à d'autres réseaux et comptes.
7. Surveillez avant de l'appliquer dans les comptes de production.

Conception avec défense en profondeur

Utilisez les politiques AWS Sign-In basées sur les ressources et les politiques de contrôle des ressources comme couche dans le cadre d'une stratégie de sécurité plus large. AWS Sign-In les politiques limitent l'accès à la console en fonction de l'emplacement du réseau et de l'identité

principale. Combinez-les avec d'autres types de politiques pour créer des contrôles d'accès complets :

- AWS Sign-In politiques (politiques basées sur les ressources et RCP) : limitez l'accès à la console en fonction de l'emplacement du réseau et de l'identité principale avant, pendant et après l'authentification.
- Politiques IAM : contrôlez les actions que les utilisateurs peuvent effectuer après s'être connectés.
- Politiques de contrôle des services (SCP) : appliquez des garanties d'autorisation à l'échelle de l'organisation à tous les principaux.
- Politiques relatives aux points de terminaison VPC : contrôlez les services et les comptes accessibles via les points de terminaison VPC.

Surveiller et auditer en permanence

AWS CloudTrail enregistre automatiquement toutes les évaluations des AWS Sign-In politiques et les modifications de configuration. Consultez ces CloudTrail événements dans l'historique des événements pendant 90 jours maximum. Pour une rétention plus longue, transmettez les événements à Amazon S3 en créant un suivi (voir Création d'un suivi). Pour des alertes en temps réel, créez des EventBridge règles Amazon adaptées aux AWS Sign-In événements, configurez votre journal pour qu'il soit envoyé à un groupe de CloudWatch journaux pour les alarmes basées sur des filtres métriques, ou transférez les événements vers votre solution SIEM existante.

Cas d'utilisation

Application du périmètre du réseau

Limitez l'accès à la console aux VPC d'entreprise ou aux plages d'adresses IP approuvées. Utilisez des politiques basées sur les ressources pour les comptes individuels ou des politiques de contrôle des ressources (RCP) pour les appliquer à l'échelle de l'organisation afin de garantir que les utilisateurs ne peuvent se connecter qu'à partir d'emplacements réseau fiables, empêchant ainsi tout accès non autorisé depuis des réseaux publics ou non fiables.

Exemple de scénario : une entreprise a besoin que tous les accès à la console proviennent de son réseau d'entreprise ou de ses AWS VPC approuvés. Ils configurent une politique basée sur les ressources pour un compte unique, ou un RCP au sein de leur organisation, qui refuse l'accès à tous les autres réseaux tout en maintenant un accès de restauration d'urgence pour les administrateurs d'urgence.

Exigences de conformité

Respectez les exigences réglementaires en matière de contrôles d'accès basés sur le réseau. De nombreux cadres de conformité obligent les entreprises à restreindre l'accès aux systèmes sensibles en fonction de l'emplacement du réseau. AWS Sign-In les politiques fournissent des contrôles vérifiables et exécutoires qui démontrent la conformité à ces exigences.

Exemple de scénario : une société de services financiers doit se conformer aux réglementations exigeant l'accès à la console uniquement à partir de réseaux approuvés. Ils utilisent les RCP pour appliquer les restrictions du réseau à l'échelle de l'organisation et tenir des AWS CloudTrail journaux comme preuve de conformité.

Multi-account gouvernance

Mettez en œuvre des politiques d'accès à la console cohérentes dans l'ensemble des organisations AWS. Utilisez les RCP pour appliquer les restrictions réseau standard à tous les comptes membres, garantissant ainsi une posture de sécurité cohérente sans nécessiter de configuration individuelle au niveau du compte.

Exemple de scénario : une entreprise possédant plus de 100 AWS comptes utilise les RCP pour appliquer une politique exigeant que tous les accès à la console proviennent des points de terminaison VPC au sein de son organisation, confirmant ainsi la cohérence des contrôles réseau sur tous les comptes.

Third-party contrôle d'accès

Accordez un accès temporaire à la console aux partenaires ou sous-traitants de réseaux spécifiques. Organisations peuvent créer un accès à la console limité dans le temps et limité au réseau pour les parties externes sans compromettre le niveau de sécurité global.

Exemple de scénario : une entreprise doit accorder à un cabinet de conseil un accès temporaire à la console. Ils créent une politique basée sur les ressources qui autorise l'accès uniquement à partir des plages d'adresses IP connues du cabinet de conseil et uniquement pour les rôles IAM attribués aux consultants.

Restreindre l'accès à la console à des utilisateurs spécifiques

Autorisez uniquement un ensemble défini de principes à se connecter au AWS Management Console, et refusez tous les autres, quel que soit l'emplacement du réseau. Cela est utile pour les clients qui n'utilisent pas de points de terminaison VPC et qui souhaitent des restrictions de console basées sur l'identité. Les principaux auxquels la connexion à la console est refusée

conservent leur accès programmatique ; AWS Sign-In les politiques limitent uniquement la connexion à la console, et seuls les principaux que vous exemptez peuvent se connecter.

Exemple de scénario : une entreprise souhaite que seuls ses administrateurs utilisent la console. Ils configurent un RCP qui refuse la connexion à la console pour tous les principaux, à l'exception des ARN principaux de l'administrateur. Un rôle d'instance Amazon EC2 doté d'informations d'identification valides ne peut pas se connecter à la console, car il ne s'agit pas d'un rôle principal exempté, même s'il conserve ses autorisations de programmation. Cela résout le cas courant d'utilisation des informations d'identification du rôle d'instance pour la connexion à la console.

Résolution des problèmes liés au contrôle d'accès à

Je ne peux pas me connecter en raison de l'état du réseau dans les politiques basées sur les Sign-in ressources

L'un des messages d'erreur suivants peut s'afficher lorsque l'accès est refusé par une AWS Sign-In politique :

- « Vos informations d'authentification sont incorrectes. Veuillez réessayer. » (refus de pré-authentification par une politique basée sur les ressources)
- « Échec de l'authentification Demande non valide » (refus de pré-authentification par le RCP)
- « Échec de l'authentification : pour accéder à ce compte, connectez-vous depuis un autre réseau ou contactez votre administrateur pour plus d'informations » (refus après l'authentification)

Si vous constatez l'une de ces erreurs et pensez que votre accès devrait être autorisé, contactez votre AWS administrateur. Ils peuvent consulter CloudTrail les journaux pour détecter les `ConsoleLogin` événements portant la mention `errorMessage` « Autorisation refusée en raison d'une politique basée sur les ressources » ou « Autorisation refusée en raison d'une politique de contrôle des ressources » afin d'identifier la déclaration de politique refusant l'accès.

Causes possibles :

- Votre adresse IP source ne se trouve pas dans la plage CIDR autorisée.
- Vous n'êtes pas connecté au VPC ou au point de terminaison VPC requis.
- Vous accédez à un point de connexion régional qui ne correspond pas à la région prévue dans la politique.

- Votre ARN principal n'est pas correctement répertorié dans les principaux exclus de la politique.
- La politique a été récemment mise à jour et le changement n'a pas encore été répliqué à l'échelle mondiale.

Résolution :

- Vérifiez que vous êtes connecté à votre réseau d'entreprise ou à votre VPN.
- Vérifiez que vous accédez via le point de terminaison VPC approprié si des restrictions basées sur les points de terminaison VPC sont configurées.
- Contactez votre AWS administrateur pour vérifier la configuration des politiques et vérifier quels réseaux sont autorisés.
- Si vous êtes configuré en tant que principal exclu, vérifiez que votre ARN principal est correctement configuré dans la liste des principaux exclus.
- Si des modifications de politique ont été récemment apportées, attendez quelques minutes que la réplication globale soit terminée.

Pour les administrateurs diagnostiquant ce problème :

- Consultez AWS CloudTrail les journaux pour détecter les événements d'évaluation des politiques afin d'identifier la déclaration de politique qui a refusé l'accès.
- `aws signin get-resource-policy`À utiliser pour revoir la configuration de la politique actuelle.
- Vérifiez que l'emplacement réseau de l'utilisateur correspond aux conditions de la politique.
- Vérifiez que les principaux exclus sont correctement configurés si l'utilisateur doit être exempté des restrictions réseau.

L'accès à mon compte est bloqué après avoir activé l'autorisation de la console

Si vous avez configuré l'autorisation de console et que vous ne pouvez plus accéder à votre compte, il se peut que vous n'ayez pas configuré les principaux exclus avant d'appliquer la politique.

Il existe plusieurs moyens de récupérer l'accès, en fonction du type de compte et des informations d'identification disponibles.

Option 1 : Utiliser l'accès par programmation (AWS CLI ou SDK)

Les politiques d'autorisation de console s'appliquent uniquement à la connexion à la console interactive. Ils ne s'appliquent pas aux demandes d'API signées avec SigV4. Si vous disposez d'un accès programmatique (par exemple, des clés d'accès existantes, un rôle multicompte), utilisez-le pour appeler `signin:DeleteConsoleAuthorizationConfiguration` et supprimer la politique de restriction. Les informations d'identification que vous utilisez doivent être autorisées à appeler`signin:DeleteConsoleAuthorizationConfiguration`. La politique `AWSSignInResourcePolicyManagement` gérée inclut cette autorisation. AWS recommande des informations d'identification temporaires plutôt que des clés d'accès utilisateur IAM à long terme. Pour les comptes membres, les administrateurs des comptes de gestion peuvent `OrganizationAccountAccessRole` accéder au compte membre pour obtenir des informations d'identification temporaires. Ce rôle n'est pas créé automatiquement dans les comptes invités à rejoindre l'organisation.

```
aws signin delete-console-authorization-configuration \
  --target-id <your-aws-account-id> \
  --region us-east-1
```

Ou supprimez des déclarations d'autorisation spécifiques :

```
# First, list statements to get the statement ID
aws signin list-resource-permission-statements \
  --region us-east-1

# Then delete the problematic statement
aws signin delete-resource-permission-statement \
  --statement-id <statement-id> \
  --region us-east-1
```

Option 2 : Contacter le AWS Support

Si vous ne disposez pas d'un accès programmatique et que vous ne pouvez pas utiliser le `OrganizationAccountAccessRole` pour accéder au compte, contactez le AWS Support pour lancer le processus de rétablissement du verrouillage.

Le processus de restauration fonctionne comme suit :

1. Si vous ne parvenez pas à résoudre le problème à l'aide des options ci-dessus, ouvrez un dossier d'assistance auprès du AWS Support Center. AWS Support vérifiera votre identité

avant d'examiner votre compte. Les méthodes de vérification peuvent inclure la confirmation de l'adresse e-mail du compte utilisateur root, la réponse à un appel de vérification téléphonique ou les réponses aux questions de sécurité du compte.

2. AWS Support confirme que le problème d'accès à la console est dû à un verrouillage politique basé sur les ressources.
3. AWS Support partage un lien vers le portail de reprise. Utilisez ce lien pour vous connecter avec un responsable IAM du compte `signin:DeleteConsoleAuthorizationConfiguration` autorisé. Cette autorisation permet au principal de supprimer la configuration d'autorisation de console à l'origine du verrouillage.

> **Important**
>
> Le portail de restauration supprime l'intégralité de la configuration d'autorisation de console pour le compte, y compris toutes les déclarations d'autorisation des ressources. Le portail de restauration n'autorise pas la reconfiguration des politiques basées sur les AWS Sign-In ressources.

Le lien du portail de restauration expire 72 heures après son partage par le AWS Support. Si vous n'effectuez pas la restauration dans cette fenêtre, contactez le AWS Support pour relancer le processus.

Une fois l'accès rétabli :

- Passez en revue et mettez à jour vos déclarations d'autorisation des ressources afin d'inclure les principaux exclus correctement configurés.
- Testez l'accès à la console depuis les réseaux attendus avant de réactiver l'autorisation de la console.
- Documentez vos procédures de recouvrement pour référence future.

Les modifications que j'apporte ne sont pas toujours visibles immédiatement

Les modifications de politique sont répliquées à l'échelle mondiale, mais la réplication peut prendre quelques minutes.

Résolution :

- Attendez quelques minutes après avoir modifié les règles pour que la réplication globale soit terminée.
- Vérifiez vos modifications à l'aide de la `get-resource-policy` commande :

```
aws signin get-resource-policy --region <your-region>
```

- Consultez les AWS CloudTrail journaux pour détecter les événements d'évaluation des politiques afin de confirmer que la nouvelle politique est en cours d'évaluation.
- Vérifiez que vous utilisez la bonne région pour vos opérations (les opérations d'écriture doivent utiliser`us-east-1`).
- Si vous utilisez des conditions basées sur les points de terminaison VPC, vérifiez que les politiques des points de terminaison VPC sont également correctement configurées.

Problèmes courants liés à la réplication des politiques :

- Page de connexion mise en cache : les navigateurs peuvent mettre en cache la page de connexion. Videz le cache de votre navigateur ou utilisez une fenêtre de navigation privée pour tester les modifications apportées aux règles.
- Déclarations contradictoires : si vous avez plusieurs déclarations d'autorisation, vérifiez qu'elles ne sont pas en conflit les unes avec les autres. `get-resource-policy`À utiliser pour revoir la politique consolidée.
- Politiques de point de terminaison VPC : les AWS Sign-In politiques fonctionnent conjointement avec les politiques de point de terminaison VPC. Les deux doivent autoriser l'accès souhaité.

AWS Sign-In référence des clés de condition

Cette page répertorie les clés de condition que vous pouvez utiliser dans les politiques AWS Sign-In basées sur les ressources et les politiques de contrôle des ressources (RCP), et indique la phase d'évaluation et les actions auxquelles chaque clé s'applique. Seule `signin:PrincipalArn` est spécifique à AWS Sign-In ; les autres sont des clés de condition AWS globales. Pour les définitions des clés globales, voir les clés contextuelles des conditions AWS globales.

Pour obtenir la liste complète des actions et des clés de condition dans la référence d'autorisation de service, voir Actions, ressources et clés de condition pour AWS Sign-In.

Network-based clés de condition

Ces clés de condition vérifient l'origine de la demande. AWS Sign-In les évalue pour toutes les AWS Sign-In actions (`signin:Authenticate`,`signin:AuthorizeOAuth2Access`, et`signin:CreateOAuth2Token`) dans les politiques basées sur les ressources et les RCP.

Network-based clés de condition

Clé de condition	Opérateurs	Description	Règles d'utilisation
`aws:SourceIp`	`IpAddress` , `NotIpAddress`	Adresse IP publique ou plage d'adresses CIDR	Absent lorsqu'une demande utilise un point de terminaison VPC. Utilisez des `IfExists` opérateurs lorsque vous combinez VPC-based des conditions dans la même instruction.
`aws:SourceVpc`	`StringEquals` , `StringNotEquals`	ID VPC () `vpc-xxxxxxxx`	Présent uniquement lorsqu'une demande utilise un point de terminaison VPC. Utilisez avec `aws:RequestedRegion` pour éviter toute collision

Clé de condition	Opérateurs	Description	Règles d'utilisation
			d'identifiants VPC entre régions.
`aws:SourceVpce`	`StringEquals`, `StringNotEquals`	ID de point de terminaison VPC () `vpce-xxxxxxxx`	Présent uniquement lorsqu'une demande utilise un point de terminaison VPC.
`aws:VpcSourceIp`	`IpAddress`, `NotIpAddress`	IP privée au sein du VPC	Utilisez toujours la clé de `aws:VpcSourceIp` condition avec les clés de `aws:SourceVpce` condition `aws:SourceVpc` ou.
`aws:RequestedRegion`	`StringEquals`, `StringNotEquals`	Code de AWS région cible	Recommandé lors de l'utilisation `aws:SourceVpc` pour éviter les collisions d'identifiants VPC entre régions. Plusieurs régions peuvent être spécifiées.

Important

Une seule demande contient soit `aws:SourceIp` (réseau public) soit `aws:SourceVpc` (point de terminaison VPC), mais pas les deux. Lorsque vous rédigez des politiques de refus couvrant les deux chemins, utilisez des `IfExists` opérateurs (par exemple`NotIpAddressIfExists`) ou créez des instructions distinctes.

Identity-based clés de condition

Ces clés de condition vérifient qui fait la demande. Ils ne sont disponibles que pour les actions post-authentification (`signin:AuthorizeOAuth2Accessetsignin:CreateOAuth2Token`), pour lesquelles l'identité principale a été établie.

Identity-based clés de condition

Clé de condition	Opérateurs	Description	Exemples
`aws:PrincipalArn`	`ArnEquals` , `ArnLike`, `ArnNotEquals` , `StringEquals` , `StringLike`	ARN du principal IAM authentifié	`arn:aws:iam::123456789012:user/alice` , `arn:aws:iam::123456789012:role/Admin`
`aws:PrincipalAccount`	`StringEquals` , `StringNotEquals`	AWS numéro de compte du mandant	`123456789012`

Service-specific clé de condition : connexion : PrincipalArn

La clé de condition suivante est spécifique à la clé globale AWS Sign-In et n'est pas une AWS clé globale. Il n'est disponible que lors de l'évaluation préalable à l'authentification. `signin:PrincipalArn`À utiliser pour identifier le principal initiateur de la connexion avant la fin de l'authentification. Il s'agit de l'équivalent de pré-authentification de`aws:PrincipalArn`, qui n'est disponible qu'après l'authentification.

Opérateurs

Opérateurs ARN (`ArnEquals`,`ArnLike`,`ArnNotEquals`,`ArnNotLike`) et opérateurs de chaîne (`StringEquals`,`StringLike`).

Disponibilité

AWS Sign-In inclut cette clé dans le contexte de la demande pendant la phase de pré-authentification (l'`signin:Authenticate`action). Il n'est pas disponible pour les actions post-authentification (`signin:AuthorizeOAuth2Accessetsignin:CreateOAuth2Token`).

Type de données

ARN. Utilisez des opérateurs ARN plutôt que des opérateurs de chaîne.

Type de la valeur

Single-valued.

Pris en charge dans

Resource-based politiques et RCP.

Utilisez les opérateurs ARN pour comparer les valeurs. Vous pouvez spécifier les types principaux suivants :

- Compte AWS utilisateur root (`arn:aws:iam::123456789012:root`)
- Utilisateur IAM () `arn:aws:iam::123456789012:user/`*`user-name`*
- Rôle IAM () `arn:aws:iam::123456789012:role/`*`role-name`*

Cas d'utilisation : exemptez une identité principale exclue des restrictions du réseau, empêchant ainsi le verrouillage tout en appliquant les contrôles réseau pour toutes les autres tentatives d'accès.

Exemple — Refuser l'accès préalable à l'authentification depuis des réseaux non autorisés, sauf pour l'utilisateur root :

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Principal": { "AWS": "*" },
      "Action": ["signin:Authenticate"],
      "Resource": "*",
      "Condition": {
        "ArnNotEquals": {
```

```
          "signin:PrincipalArn": "arn:aws:iam::123456789012:root"
        },
        "NotIpAddress": {
          "aws:SourceIp": "203.0.113.0/24"
        },
        "StringEquals": {
          "aws:ResourceAccount": "123456789012"
        }
      }
    },
    {
      "Effect": "Deny",
      "Principal": { "AWS": "*" },
      "Action": ["signin:CreateOAuth2Token", "signin:AuthorizeOAuth2Access"],
      "Resource": "*",
      "Condition": {
        "ArnNotEquals": {
          "aws:PrincipalArn": "arn:aws:iam::123456789012:root"
        },
        "NotIpAddress": {
          "aws:SourceIp": "203.0.113.0/24"
        },
        "StringEquals": {
          "aws:ResourceAccount": "123456789012"
        }
      }
    }
  ]
}
```

Cette politique interdit l'accès à la console depuis l'extérieur de la plage d'`203.0.113.0/24`adresses IP, sauf pour l'utilisateur root du compte. L'instruction de pré-authentification est utilisée `signin:PrincipalArn` pour exempter l'utilisateur root avant la fin de l'authentification. L'instruction de post-authentification est utilisée `aws:PrincipalArn` pour exempter le même principal après authentification, lors de l'échange de jetons OAuth. Consultez Exemples de politiques.

Disponibilité de la clé de condition par action

Disponibilité de la clé de condition par action

Clé de condition	Se connecter : authentifier	connexion : Authorize OAuth2Access	connexion : CreateOAuth2Token
`aws:SourceIp`	Oui	Oui	Oui
`aws:SourceVpc`	Oui	Oui	Oui
`aws:SourceVpce`	Oui	Oui	Oui
`aws:VpcSourceIp`	Oui	Oui	Oui
`aws:RequestedRegion`	Oui	Oui	Oui
`aws:PrincipalArn`	–	Oui	Oui
`aws:PrincipalAccount`	–	Oui	Oui
`signin:PrincipalArn`	Oui	–	–

> **Note**
>
> L'`signin:CreateAccount`action est utilisée exclusivement dans les politiques de point de terminaison VPC pour l'accès privé à la console et n'est pas disponible pour les politiques basées sur les ressources ou les RCP. Aucune clé de condition spécifique au service n'y est associée. Voir Accès privé à la console.

Informations connexes

- Contrôle de l'accès à la console à l'aide de politiques basées sur les ressources et de politiques de contrôle des ressources
- AWS Management Console Accès privé
- AWS Clés de contexte de condition globale
- Actions, ressources et clés de condition pour AWS Sign-In

Connectez-vous à votre AWS portail d'accès

Un utilisateur d'IAM Identity Center est membre de AWS Organizations. Un utilisateur d'IAM Identity Center peut accéder à plusieurs Comptes AWS applications professionnelles en se connectant à votre portail d' AWS accès à l'aide d'une URL de connexion spécifique. Pour plus d'informations sur l'URL de connexion spécifique, consultezAWS portail d'accès.

Avant de vous connecter en Compte AWS tant qu'utilisateur dans IAM Identity Center, collectez les informations requises suivantes.

- Nom d'utilisateur de l'entreprise
- Mot de passe d'entreprise
- URL de connexion spécifique

> **Note**
>
> Une fois connecté, votre session AWS au portail d'accès est valide pendant 8 heures. Vous devez vous reconnecter au bout de 8 heures.

Pour vous connecter à votre AWS portail d'accès

1. Dans la fenêtre de votre navigateur, collez l'URL de connexion qui vous a été fournie par e-mail, par exemple le format `https://your_subdomain.awsapps.com/start` d'URL à double pile. `https://[IAM Identity Center instance ID].portal.[Region].app.aws` Ensuite, appuyez sur Entrée.
2. Connectez-vous à l'aide des informations d'identification de votre entreprise (comme un nom d'utilisateur et un mot de passe).

   > **Note**
   >
   > Si votre administrateur vous a envoyé un mot de passe à usage unique (OTP) par e-mail et que c'est la première fois que vous vous connectez, saisissez-le. Une fois connecté, vous devez créer un nouveau mot de passe pour les connexions futures.

3. Si un code de vérification vous est demandé, consultez vos e-mails pour le trouver. Copiez et collez ensuite le code dans la page de connexion.

   > **Note**
   >
   > Les codes de vérification sont généralement envoyés par e-mail, mais le mode de livraison peut varier. Si vous n'en avez pas reçu un dans votre e-mail, contactez votre administrateur pour obtenir des informations sur votre code de vérification.

4. Si la MFA est activée pour votre utilisateur dans IAM Identity Center, vous vous authentifiez à l'aide de cette fonctionnalité.
5. Après l'authentification, vous pouvez accéder à toutes Compte AWS les applications qui apparaissent sur le portail.

   a. Pour vous connecter, AWS Management Console choisissez l'onglet Comptes et sélectionnez le compte individuel à gérer.

      Le rôle de votre utilisateur s'affiche. Choisissez le nom du rôle du compte pour ouvrir le AWS Management Console. Choisissez les touches d'accès pour obtenir les informations d'identification pour l'accès par ligne de commande ou par programmation.

   b. Choisissez l'onglet Applications pour afficher les applications disponibles et choisissez l'icône de l'application à laquelle vous souhaitez accéder.

La connexion en tant qu'utilisateur dans IAM Identity Center vous fournit des informations d'identification vous permettant d'accéder aux ressources pendant une durée définie, appelée session. Par défaut, un utilisateur peut être connecté à un compte Compte AWS pendant 8 heures. L'administrateur du centre d'identité IAM peut spécifier une durée différente, allant d'un minimum de 15 minutes à un maximum de 90 jours. Une fois votre session terminée, vous pouvez vous reconnecter.

Informations supplémentaires

Pour plus d'informations sur les utilisateurs d'IAM Identity Center, consultez les ressources suivantes.

- Pour une présentation d'IAM Identity Center, voir Qu'est-ce qu'IAM Identity Center ?
- Pour plus de détails sur votre portail AWS d'accès, consultez la section Utilisation du portail AWS d'accès.

- Pour plus de détails sur les sessions IAM Identity Center, consultez la section Authentifications des utilisateurs.
- Pour obtenir des instructions détaillées sur la façon de réinitialiser votre mot de passe utilisateur IAM Identity Center, consultezJ'ai oublié le mot de passe IAM Identity Center pour mon Compte AWS.
- Si vous ou votre organisation implémentez le filtrage des adresses IP ou des domaines, vous devrez peut-être autoriser les domaines sur liste pour créer et utiliser votre portail AWS d'accès. IAM Identity Center prend en charge les points de terminaison IPv4 et à double pile. Si votre réseau utilise IPv6, utilisez les domaines de point de terminaison à double pile. Pour en savoir plus sur l'autorisation de mettre en vente des domaines, consultezDomaines à ajouter à votre liste d'autorisations.

Connectez-vous via le AWS Command Line Interface

Vous devez définir la manière dont il s' AWS CLI authentifie auprès AWS de. Choisissez la méthode qui correspond le mieux à votre flux de travail et à vos exigences de sécurité.

- Connectez-vous avec les informations d'identification de la console (recommandé)si vous utilisez root, des utilisateurs IAM ou une fédération avec IAM pour accéder au AWS compte.
- Connectez-vous avec les informations d'identification IAM Identity Centersi vous utilisez Identity Center pour accéder au AWS compte.

Connectez-vous avec les informations d'identification de la console (recommandé)

Cette méthode d'authentification vous permet d'utiliser les informations d'identification de votre console avec le AWS CLI, ce qui vous permet de démarrer facilement AWS par programmation quelques minutes après la création du compte. Vous pouvez obtenir des informations d'identification temporaires qui fonctionnent parfaitement avec les outils de développement locaux tels que AWS CLI, AWS SDKs et Outils AWS pour PowerShell.

Conditions préalables

- Installez le AWS CLI. Pour plus d'informations, consultez Installation ou mise à jour de la version la plus récente de l' AWS CLI. Une version minimale de 2.32.0 est requise pour utiliser la `aws login` commande.
- Accès pour se connecter en AWS Management Console tant qu'utilisateur root, utilisateur IAM ou via une fédération avec IAM. Si vous utilisez IAM Identity Center, rendez-vous Connectez-vous avec les informations d'identification IAM Identity Center plutôt sur.
- Assurez-vous que l'identité IAM dispose des autorisations appropriées. Associez la politique SignInLocalDevelopmentAccessgérée à votre utilisateur, rôle ou groupe IAM. Si vous vous connectez en tant qu'utilisateur root, aucune autorisation supplémentaire n'est requise.

Pour vous connecter avec les informations d'identification de la console

1. Exécutez la commande suivante pour démarrer le processus d'authentification par navigateur :

```
$ aws login
```

La `aws login` commande prend en charge plusieurs paramètres facultatifs :

- `aws login --remote`- Pour l'authentification multi-appareils lorsque votre appareil n'est pas compatible avec un navigateur

> **Note**
>
> Vous pouvez contrôler l'accès à l'authentification sur un même appareil (`aws login`) et sur plusieurs appareils (`aws login --remote`). Utilisez la ressource suivante ARNs dans toute politique IAM pertinente.
>
> - `arn:aws:signin:region:account-id:oauth2/public-client/localhost`— Utilisez cet ARN pour l'authentification sur le même appareil avec. `aws login`
> - `arn:aws:signin:region:account-id:oauth2/public-client/remote`— Utilisez cet ARN pour l'authentification multi-appareils avec`aws login --remote`.

- `aws login --profile profile-name`- Pour s'authentifier avec un profil spécifique
- `aws login --region region`- Pour s'authentifier dans une région spécifique

2. Suivez les instructions de votre terminal. La commande ouvre automatiquement votre navigateur par défaut et vous guide tout au long du processus d'authentification. Une fois l'authentification réussie, votre AWS CLI session sera valide pendant 12 heures au maximum.
3. Pour terminer votre session, utilisez :

```
$ aws logout
```

Si vous accédez aux AWS services par programmation en utilisant Outils AWS pour PowerShell, veuillez consulter Authentification des outils AWS pour AWS. PowerShell Si vous utilisez AWS SDKs, veuillez consulter Authentification et accès à l'aide d'AWS SDKs et des outils.

Connectez-vous avec les informations d'identification IAM Identity Center

Le portail AWS d'accès permet aux utilisateurs d'IAM Identity Center de sélectionner Compte AWS et d'obtenir facilement des informations d'identification de sécurité temporaires pour le AWS CLI. Pour plus d'informations sur la façon d'obtenir ces informations d'identification, consultezDisponibilité de la région pour ID de constructeur AWS. Vous pouvez également configurer le AWS CLI directement pour authentifier les utilisateurs auprès d'IAM Identity Center.

Pour vous connecter avec les informations d'identification IAM Identity Center

1. Vérifiez que vous avez rempli les prérequis.
2. Si vous vous connectez pour la première fois, configurez votre profil à l'aide de l'`aws configure ssoassistant`.
3. Après avoir configuré votre profil, exécutez la commande suivante, puis suivez les instructions de votre terminal :

```
$ aws sso login --profile my-profile
```

Informations supplémentaires

Pour plus d'informations sur la connexion à l'aide de la ligne de commande, consultez les ressources suivantes.

- Pour plus d'informations sur l'utilisation des informations d'identification de votre console pour vous connecter à AWS des fins de développement local, consultez Authentification et informations d'accès pour l'interface de ligne de commande AWS.
- Pour plus d'informations sur le processus de AWS CLI connexion, voir Authentification à l'aide d'informations d'identification à court terme pour le. AWS CLI
- Pour plus de détails sur la configuration d'IAM Identity Center, voir Configuration du AWS CLI pour utiliser IAM Identity Center.

Connectez-vous en tant qu'identité fédérée

Une identité fédérée est un utilisateur qui peut accéder à Compte AWS des ressources sécurisées avec des identités externes. Les identités externes peuvent provenir d'un magasin d'identités d'entreprise (tel que LDAP ou Windows Active Directory) ou d'une partie tierce (Login with Amazon, Facebook ou Google, par exemple). Les identités fédérées ne se connectent pas au portail AWS Management Console ou n' AWS accèdent pas. Le type d'identité externe utilisé détermine la manière dont les identités fédérées se connectent.

Les administrateurs doivent créer une URL personnalisée qui inclut`https://signin.aws.amazon.com/federation`. Pour plus d'informations, voir Activation de l'accès des courtiers d'identité personnalisés au AWS Management Console.

> **Note**
>
> Votre administrateur crée des identités fédérées. Contactez votre administrateur pour plus de détails sur la procédure de connexion en tant qu'identité fédérée.

Pour plus d'informations sur les identités fédérées, consultez À propos de la fédération des identités Web.

Connectez-vous avec ID de constructeur AWS

ID de constructeur AWS est un profil personnel qui donne accès à certains outils et services, notamment Amazon CodeCatalyst, Amazon Q Developer AWS Training et Certification. ID de constructeur AWS vous représente en tant qu'individu et est indépendant des informations d'identification et des données que vous pourriez avoir dans AWS des comptes existants. Comme les autres profils personnels, ID de constructeur AWS il vous accompagne au fur et à mesure que vous progressez dans vos objectifs personnels, éducatifs et professionnels.

Vos ID de constructeur AWS compléments à ceux Comptes AWS que vous possédez déjà ou que vous souhaitez créer. Alors qu'un Compte AWS agit comme un conteneur pour les AWS ressources que vous créez et fournit une limite de sécurité pour ces ressources, vous vous ID de constructeur AWS représente en tant qu'individu. Pour de plus amples informations, veuillez consulter ID de constructeur AWS et autres AWS informations d'identification.

ID de constructeur AWS est gratuit. Vous ne payez que pour les AWS ressources que vous consommez dans votre Comptes AWS. Pour plus d'informations sur la tarification, consultez Tarification d'AWS.

Si vous ou votre organisation implémentez le filtrage des adresses IP ou des domaines, vous devrez peut-être autoriser les domaines à créer et à utiliser un ID de constructeur AWS. Pour en savoir plus sur l'autorisation de mettre en vente des domaines, consultezDomaines à ajouter à votre liste d'autorisations.

> **Note**
>
> AWS Le Builder ID est distinct de votre abonnement à AWS Skill Builder, un centre de formation en ligne où vous pouvez apprendre auprès d' AWS experts et développer des compétences en matière de cloud en ligne. Pour plus d'informations sur AWS Skill Builder, consultez AWS Skill Builder.

Rubriques

- AWS outils et services qui utilisent ID de constructeur AWS
- Modifiez votre ID de constructeur AWS profil
- Changez votre ID de constructeur AWS mot de passe
- Supprimez toutes les sessions actives pour votre ID de constructeur AWS
- Supprimez votre ID de constructeur AWS
- Gérer l'authentification ID de constructeur AWS multifactorielle (MFA)
- Confidentialité et données dans ID de constructeur AWS
- ID de constructeur AWS et autres AWS informations d'identification

Pour vous connecter avec ID de constructeur AWS

1. Accédez au ID de constructeur AWS profil ou à la page de connexion de l' AWS outil ou du service auquel vous souhaitez accéder. Par exemple, pour accéder à Amazon CodeCatalyst, rendez-vous surhttps://codecatalyst.aws.
2. Choisissez comment vous connecter à votre ID de constructeur AWS
   - J'ai déjà un compte
   - J'ai un compte Google
   - J'ai un compte Apple
   - J'ai un GitHub compte
   - J'ai un compte Amazon

J'ai déjà un compte

1. Pour les comptes existants, saisissez l'adresse e-mail que vous avez utilisée pour créer votre compte ID de constructeur AWS et choisissez Se connecter.
2. Entrez l'adresse e-mail que vous avez utilisée pour créer votre ID de constructeur AWS compte et choisissez Se connecter.
3. Sur la ID de constructeur AWS page Connectez-vous avec votre nom de passe, saisissez votre mot de passe.
4. (Facultatif) Si vous souhaitez que les futures connexions à partir de cet appareil ne nécessitent pas de vérification supplémentaire, cochez la case à côté de Cet appareil est fiable.
5. Sélectionnez Continuer.

6. Si une page de vérification supplémentaire est requise, suivez les instructions de votre navigateur pour fournir le code ou la clé de sécurité requis.

> **Note**
>
> Pour votre sécurité, nous analysons votre navigateur de connexion, votre localisation et votre appareil. Si vous nous dites de faire confiance à cet appareil, vous n'aurez pas à fournir de code d'authentification multifactorielle (MFA) à chaque fois que vous vous connecterez. Pour de plus amples informations, veuillez consulter Appareils approuvés.

J'ai un compte Google

Si votre compte Google est déjà associé à une ID de constructeur AWS, vous devez utiliser une adresse e-mail différente pour vous connecter à une application. Pour de plus amples informations, veuillez consulter Je n'arrive pas à me connecter avec Google.

1. Pour vous connecter à votre compte Google ID de constructeur AWS, choisissez Continuer avec Google.
2. Sur la page Se connecter avec Google, saisissez les informations de votre compte Google pour vous connecter.
3. Choisissez Continuer pour charger la page d'accueil de AWS l'application.

J'ai un compte Apple

Si votre compte Apple est déjà associé à une ID de constructeur AWS, vous devez utiliser une adresse e-mail différente pour vous connecter à une application. Pour de plus amples informations, veuillez consulter Je n'arrive pas à me connecter avec Apple.

1. Pour vous connecter à votre compte Apple ID de constructeur AWS, choisissez Continuer avec Apple.
2. Sur la page Se connecter avec Apple, entrez les informations de votre compte Apple pour vous connecter.
3. Choisissez Continuer pour charger la page d'accueil de AWS l'application.

J'ai un GitHub compte

Si votre GitHub compte est déjà associé à une ID de constructeur AWS, vous devez utiliser une adresse e-mail différente pour vous connecter à une application. Pour de plus amples informations, veuillez consulter Je n'arrive pas à me connecter avec GitHub.

1. Pour vous connecter à votre GitHub compte ID de constructeur AWS, choisissez Continuer avec GitHub.
2. Sur la GitHub page Se connecter avec, entrez les informations relatives à votre GitHub compte pour vous connecter.
3. Choisissez Continuer pour charger la page d'accueil de AWS l'application.

J'ai un compte Amazon

Si votre compte Amazon est déjà associé à une ID de constructeur AWS, vous devez utiliser une adresse e-mail différente pour vous connecter à une application. Pour de plus amples informations, veuillez consulter Je n'arrive pas à me connecter avec Amazon.

1. Pour vous connecter à votre compte Amazon ID de constructeur AWS, choisissez Continuer avec Amazon.
2. Sur la page Se connecter avec Amazon, saisissez les informations de votre compte Amazon pour vous connecter.
3. Choisissez Continuer pour charger la page d'accueil de AWS l'application.

Disponibilité de la région pour ID de constructeur AWS

ID de constructeur AWS est disponible dans les versions suivantes Régions AWS. Les applications utilisées ID de constructeur AWS peuvent fonctionner dans d'autres régions.

Nom	Code
USA Est (Virginie du Nord)	us-east-1

Créez votre ID de constructeur AWS

Vous créez le vôtre ID de constructeur AWS lorsque vous vous inscrivez à l'un des AWS outils et services qui l'utilisent. Inscrivez-vous avec votre adresse e-mail, votre nom et votre mot de passe dans le cadre du processus d'inscription à un AWS outil ou à un service.

Votre mot de passe doit respecter les exigences suivantes :

- Les mots de passe distinguent majuscules et minuscules.
- Les mots de passe doivent comporter entre 8 et 64 caractères.
- Les mots de passe doivent contenir au moins un caractère appartenant à chacune des quatre catégories suivantes :
  - Lettres minuscules (a-z)
  - Lettres majuscules (A-Z)
  - Chiffres (0-9)
  - Caractères non alphanumériques (~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/)
- Les trois derniers mots de passe ne peuvent pas être réutilisés.
- Les mots de passe connus du public grâce à un ensemble de données divulgué par un tiers ne peuvent pas être utilisés.

> **Note**
>
> Les outils et services que vous utilisez ID de constructeur AWS vous permettent de créer et d'utiliser le vôtre en ID de constructeur AWS cas de besoin.

Pour créer votre ID de constructeur AWS

1. Accédez au ID de constructeur AWS profil ou à la page d'inscription de l' AWS outil ou du service auquel vous souhaitez accéder. Par exemple, pour accéder à Amazon CodeCatalyst, rendez-vous surhttps://codecatalyst.aws.
2. Choisissez comment créer votre ID de constructeur AWS
   - Pour utiliser votre compte Google, choisissez Continuer avec Google et suivez les instructions pour terminer le processus d'inscription. Cela permet d'ignorer les étapes 3 à 8 ci-dessous. Passez à l'étape 9.

- Pour utiliser votre compte Apple, choisissez Continuer avec Apple et suivez les instructions pour terminer le processus d'inscription. Cela permet d'ignorer les étapes 3 à 8 ci-dessous. Passez à l'étape 9.

  > **Note**
  >
  > Si vous choisissez d'activer la fonctionnalité « Masquer mon e-mail » d'iCloud+ pour vous connecter avec Apple, vous ID de constructeur AWS serez créé avec l'adresse Masquer mon e-mail désignée dans votre compte Apple au lieu de votre véritable adresse e-mail. Vous ne pourrez pas modifier cette adresse e-mail, mais vos prénom et nom de famille seront toujours modifiables. Si vous devez vous connecter à ID de constructeur AWS, vous devez utiliser votre adresse Hide My Email. ID de constructeur AWS utilisera votre adresse Hide My Email pour vous envoyer des communications par e-mail. Pour plus de détails, consultez Comment utiliser Hide My Email avec Sign in with Apple.

- Pour utiliser votre GitHub compte, choisissez Continuer avec GitHub et suivez les instructions pour terminer le processus d'inscription. Cela permet d'ignorer les étapes 3 à 8 ci-dessous. Passez à l'étape 9.
- Pour utiliser votre compte Amazon, choisissez Continuer avec Amazon et suivez les instructions pour terminer le processus d'inscription. Cela permet d'ignorer les étapes 3 à 8 ci-dessous. Passez à l'étape 9.
- Pour créer un compte avec e-mail et mot de passe, procédez comme suit.

3. Sur la ID de constructeur AWS page Créer, saisissez votre adresse e-mail. Nous vous recommandons d'utiliser une adresse e-mail personnelle.
4. Choisissez Suivant.
5. Entrez votre nom, puis choisissez Next.
6. Sur la page de vérification par e-mail, entrez le code de vérification que nous avons envoyé à votre adresse e-mail. Choisissez Vérifier. Selon votre fournisseur de messagerie, la réception de l'e-mail peut prendre quelques minutes. Vérifiez la présence du code dans vos dossiers de spam et de courrier indésirable. Si l'e-mail ne s'affiche pas au AWS bout de cinq minutes, choisissez Renvoyer le code.
7. Après avoir vérifié votre e-mail, sur la page Choisissez un mot de passe, entrez un mot de passe et confirmez le mot de passe.

8. Si un Captcha apparaît comme mesure de sécurité supplémentaire, entrez les caractères que vous voyez.
9. Choisissez Créer ID de constructeur AWS.

Appareils approuvés

Une fois que vous avez sélectionné l'option Ceci est un appareil fiable sur la page de connexion, nous considérons que toutes les futures connexions à partir de ce navigateur Web sur cet appareil sont autorisées. Cela signifie que vous n'avez pas à fournir de code MFA sur cet appareil fiable. Toutefois, si votre navigateur, vos cookies ou votre adresse IP changent, vous devrez peut-être utiliser votre code MFA pour une vérification supplémentaire.

AWS outils et services qui utilisent ID de constructeur AWS

Vous pouvez vous connecter ID de constructeur AWS pour accéder aux AWS outils et services suivants. L'accès aux fonctionnalités ou aux avantages proposés moyennant un supplément nécessite un Compte AWS.

Par défaut, lorsque vous vous connectez à un AWS outil ou à un service à l'aide de votre ID de constructeur AWS, la durée de session est de 30 jours, sauf pour Amazon Q Developer, qui a une durée de session de 90 jours. Une fois votre session terminée, vous devrez vous reconnecter.

AWS Communauté cloud

Community.aws est une plateforme créée par et pour la communauté de AWS constructeurs à laquelle vous pouvez accéder avec votre. ID de constructeur AWS C'est un endroit pour découvrir du contenu éducatif, partager vos idées et projets personnels, commenter les publications des autres et suivre vos créateurs préférés.

Amazon CodeCatalyst

Vous créerez un identifiant ID de constructeur AWS lorsque vous commencerez à utiliser Amazon CodeCatalyst et choisirez un alias qui sera associé à des activités telles que les problèmes, les validations de code et les pull requests. Invitez d'autres personnes à rejoindre votre CodeCatalyst espace Amazon, qui comprend les outils, l'infrastructure et les environnements dont votre équipe a besoin pour mener à bien votre prochain projet. Vous aurez besoin d'un Compte AWS pour déployer un nouveau projet dans le cloud.

AWS Migration Hub

Accédez AWS Migration Hub(Migration Hub) avec votre ID de constructeur AWS. Migration Hub fournit un emplacement unique pour découvrir vos serveurs existants, planifier les migrations et suivre l'état de chaque migration d'application.

Amazon Q Developer

Amazon Q Developer est un assistant conversationnel génératif alimenté par l'IA qui peut vous aider à comprendre, créer, étendre et exploiter des applications. AWS Pour plus d'informations, consultez la section What is Amazon Q Developer? du guide de l'utilisateur Amazon Q Developer.

AWS re:Post

AWS re:Postvous fournit des conseils techniques d'experts afin que vous puissiez innover plus rapidement et améliorer l'efficacité opérationnelle à l'aide de AWS services. Vous pouvez vous connecter avec votre compte ID de constructeur AWS et rejoindre la communauté sur Re:post sans carte de crédit. Compte AWS

AWS Startups

Utilisez votre ID de constructeur AWS pour rejoindre AWS des startups où vous pouvez utiliser du contenu d'apprentissage, des outils, des ressources et du soutien pour développer votre start-up AWS.

AWS Training et certification

Vous pouvez utiliser votre accès ID de constructeur AWS AWS Training à une certification qui vous permettra de développer vos AWS Cloud compétences avec AWS Skill Builder, d'apprendre auprès d' AWS experts et de valider votre expertise dans le cloud grâce à une certification reconnue par le secteur.

Kiro

Kiro est un IDE agentic qui vous aide à passer du prototype à la production grâce à un développement piloté par les spécifications. Qu'il s'agisse de tâches simples ou complexes, Kiro travaille à vos côtés pour transformer les instructions en spécifications détaillées, puis en code fonctionnel, en documents et en tests. Avec Kiro, ce que vous créez correspond exactement à vos attentes et est prêt à être partagé avec votre équipe. Les agents de Kiro vous aident à résoudre des problèmes complexes et à automatiser des tâches telles que la génération de documentation et les tests unitaires. Avec Kiro, vous pouvez construire au-delà des prototypes tout en étant aux commandes à chaque étape.

Portail d'enregistrement du site Web (WRP)

Vous pouvez utiliser votre identité ID de constructeur AWS de client et votre profil d'enregistrement permanents pour le site Web AWS de marketing. Pour vous inscrire à de nouveaux webinaires et pour voir tous les webinaires auxquels vous vous êtes inscrit ou auxquels vous avez assisté, consultez Mes webinaires.

Modifiez votre ID de constructeur AWS profil

Vous pouvez modifier les informations de votre profil à tout moment. Vous pouvez modifier l'adresse e-mail et le nom que vous avez utilisés pour créer un ID de constructeur AWS, ainsi que votre surnom. Lorsque vous utilisez des connexions sociales telles que Google ou Apple, seuls le nom et le surnom sont modifiables.

Votre nom est la façon dont vous êtes désigné dans les outils et les services lorsque vous interagissez avec les autres. Votre surnom indique la façon dont vous souhaitez être connu AWS, vos amis et les autres personnes avec lesquelles vous collaborez étroitement.

> **Note**
>
> Les outils et services que vous utilisez ID de constructeur AWS vous permettent de créer et d'utiliser le vôtre en ID de constructeur AWS cas de besoin.

Pour modifier les informations de votre profil

1. Connectez-vous à votre ID de constructeur AWS profil à l'adressehttps://profile.aws.amazon.com.
2. Choisissez Mes coordonnées.
3. Sur la page Mes informations, cliquez sur le bouton Modifier à côté de Profil.
4. Sur la page Modifier le profil, apportez les modifications souhaitées à votre nom et à votre surnom.
5. Sélectionnez Enregistrer les modifications. Un message de confirmation vert apparaît en haut de la page pour vous informer que vous avez mis à jour votre profil.

> **Note**
>
> La modification de votre nom et de votre surnom auprès de l'un de nos autres partenaires de connexion ne met pas à jour les mêmes paramètres pour votre ID de constructeur AWS.

Pour modifier vos informations de contact

1. Connectez-vous à votre ID de constructeur AWS profil à l'adressehttps://profile.aws.amazon.com.
2. Choisissez Mes coordonnées.
3. Sur la page Mes coordonnées, cliquez sur le bouton Modifier à côté de Informations de contact.
4. Sur la page Modifier les informations de contact, modifiez votre adresse e-mail.
5. Choisissez Vérifier l'adresse e-mail. Une boîte de dialogue apparaît.
6. Dans la boîte de dialogue Vérifier l'e-mail, après avoir reçu le code dans votre e-mail, saisissez-le dans le champ Code de vérification. Choisissez Vérifier.

Changez votre ID de constructeur AWS mot de passe

Votre mot de passe doit respecter les exigences suivantes :

- Les mots de passe distinguent majuscules et minuscules.
- Les mots de passe doivent comporter entre 8 et 64 caractères.
- Les mots de passe doivent contenir au moins un caractère appartenant à chacune des quatre catégories suivantes :
  - Lettres minuscules (a-z)
  - Lettres majuscules (A-Z)
  - Chiffres (0-9)
  - Caractères non alphanumériques (~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/)
- Les trois derniers mots de passe ne peuvent pas être réutilisés.

> **Note**
>
> Les modifications de mot de passe ne sont pas disponibles pour les ID de constructeur AWS comptes utilisant des connexions sociales telles que Google ou Apple. Si vous vous êtes connecté à l'aide d'un identifiant social, vous gérez votre mot de passe via votre compte de connexion sociale. Pour modifier votre mot de passe pour une connexion aux réseaux sociaux, procédez comme suit :
>
> - Pour un compte Google, voir Modifier ou réinitialiser votre mot de passe (Google).
> - Pour un compte Apple, voir Modifier le mot de passe de votre compte Apple.
> - Pour un GitHub compte, voir Mettre à jour vos informations d' GitHub accès.
> - Pour un compte Amazon, consultez Comment modifier le mot de passe Amazon.

Pour modifier votre ID de constructeur AWS mot de passe

1. Connectez-vous à votre ID de constructeur AWS profil à l'adressehttps://profile.aws.amazon.com.
2. Choisissez Security (Sécurité).
3. Sur la page Sécurité, choisissez Modifier le mot de passe. Cela vous amène à une nouvelle page.
4. Sur la page Entrez à nouveau votre mot de passe, sous Mot de passe, entrez votre mot de passe actuel. Choisissez ensuite Se connecter.
5. Sur la page Modifier votre mot de passe, sous Nouveau mot de passe, entrez le nouveau mot de passe que vous souhaitez utiliser. Ensuite, sous Confirmer le mot de passe, entrez à nouveau le nouveau mot de passe que vous souhaitez utiliser.
6. Choisissez Modifier le mot de passe. Vous êtes redirigé vers votre ID de constructeur AWS profil.

Supprimez toutes les sessions actives pour votre ID de constructeur AWS

Sous Appareils connectés, vous pouvez voir tous les appareils auxquels vous êtes actuellement connecté. Si vous ne reconnaissez pas un appareil, pour des raisons de sécurité, modifiez d'abord votre mot de passe, puis déconnectez-vous de tous les appareils. Vous pouvez vous déconnecter

de tous les appareils en supprimant toutes vos sessions actives sur la page Sécurité de votre ID de constructeur AWS.

> **Note**
>
> ID de constructeur AWS prend en charge les sessions prolongées de 90 jours pour Amazon Q Developer dans un IDE. Pour chaque nouvelle connexion à l'IDE, vous pouvez voir deux entrées de session. Lorsque vous vous déconnectez de votre IDE, vous pouvez continuer à voir les sessions IDE répertoriées sous Appareils connectés même si elles ne sont plus valides. Ces sessions disparaissent une fois les 90 jours expirés.

Pour supprimer toutes les sessions actives

1. Connectez-vous à votre ID de constructeur AWS profil à l'adressehttps://profile.aws.amazon.com.
2. Choisissez Security (Sécurité).
3. Sur la page Sécurité, choisissez Supprimer toutes les sessions actives.
4. Dans la boîte de dialogue Supprimer toutes les sessions, entrez Supprimer tout. En supprimant toutes vos sessions, vous vous déconnectez de tous les appareils auxquels vous vous êtes connecté à l'aide du vôtre ID de constructeur AWS, y compris des différents navigateurs. Choisissez ensuite Supprimer toutes les sessions.

> **Note**
>
> Lorsque vous utilisez un compte de connexion sociale tel que Google ou Apple, la suppression de ID de constructeur AWS sessions actives ne vous déconnecte pas de votre compte de connexion sociale.

Supprimez votre ID de constructeur AWS

La procédure suivante décrit comment supprimer votre ID de constructeur AWS compte.

> **Warning**
>
> Si vous supprimez le vôtre, ID de constructeur AWS vous obtiendrez les résultats suivants :

- Perte d'accès — Vous ne pouvez plus accéder aux AWS outils et services auxquels vous avez accédé auparavant ID de constructeur AWS. ID de constructeur AWS Le vôtre est distinct de tout AWS compte que vous pourriez avoir, et sa suppression ne ID de constructeur AWS fermera pas votre AWS compte.
- Suppression de contenu — Tout contenu restant associé uniquement à vous ID de constructeur AWS sera supprimé et vous ne pourrez plus accéder à votre contenu ou le récupérer à partir d'applications utilisant votre ID de constructeur AWS.
- Suppression des informations personnelles — Toutes les informations personnelles que vous avez fournies dans le cadre de la création et de l'administration de vos informations ID de constructeur AWS seront supprimées, sauf celles qui AWS peuvent conserver des informations personnelles conformément à la loi, telles que les enregistrements de votre demande de suppression ou les données sous une forme ne permettant pas de vous identifier.

  Pour en savoir plus sur la manière dont nous traitons vos informations, consultez l'avis de confidentialité d'AWS. Vous pouvez mettre à jour vos préférences AWS de communication ou vous désabonner en vous rendant dans le centre des préférences de communication AWS.
- Les comptes de connexion sociale restent inchangés — Si vous utilisez un identifiant social tel que Google ou Apple, le supprimer ID de constructeur AWS ne supprime aucun élément lié à votre compte de connexion sociale. Reportez-vous à la documentation de votre fournisseur de connexion sociale pour savoir comment supprimer ces comptes. La suppression de la ID de constructeur AWS connexion de votre compte de connexion aux réseaux sociaux ne supprime pas votre ID de constructeur AWS compte, mais vous ne pourrez plus accéder à votre ID de constructeur AWS profil.

Pour supprimer votre ID de constructeur AWS

1. Connectez-vous à votre ID de constructeur AWS profil à l'adressehttps://profile.aws.amazon.com.
2. Choisissez Confidentialité et données.
3. Sur la page Confidentialité et données, sous Supprimer ID de constructeur AWS, choisissez Supprimer ID de constructeur AWS.

4. Cochez la case à côté de chaque clause de non-responsabilité pour confirmer que vous êtes prêt à continuer.
5. Sélectionnez Supprimer ID de constructeur AWS.

Gérer l'authentification ID de constructeur AWS multifactorielle (MFA)

L'authentification multifactorielle (MFA) est un mécanisme simple et efficace pour renforcer votre sécurité. Le premier facteur, votre mot de passe, est un secret que vous mémorisez, également appelé facteur de connaissance. Les autres facteurs peuvent être des facteurs liés à la possession (quelque chose que vous possédez, comme une clé de sécurité) ou des facteurs inhérents (quelque chose que vous êtes, comme un scan biométrique). Nous vous recommandons vivement de configurer le MFA pour ajouter une couche supplémentaire à votre. ID de constructeur AWS

Vous pouvez enregistrer un authentificateur intégré et également enregistrer une clé de sécurité que vous conservez dans un endroit physiquement sécurisé. Si vous ne parvenez pas à utiliser votre authentificateur intégré, vous pouvez utiliser votre clé de sécurité enregistrée. Pour les applications d'authentification, vous pouvez également activer la fonctionnalité de sauvegarde ou de synchronisation dans le cloud dans ces applications. Cela vous permet d'éviter de perdre l'accès à votre profil si vous perdez ou cassez votre appareil MFA.

Points clés

- Nous vous recommandons d'enregistrer plusieurs appareils MFA. Si vous perdez l'accès à tous les appareils MFA enregistrés, vous ne pourrez pas récupérer votre. ID de constructeur AWS
- Nous vous recommandons de vérifier régulièrement les dispositifs MFA enregistrés pour vous assurer qu'ils sont à jour et fonctionnels. En outre, vous devez stocker ces appareils dans un endroit physiquement sûr lorsqu'ils ne sont pas utilisés.
- Si vous avez créé votre compte à l'aide de Continue with Google, vous pouvez activer l'authentification multifactorielle via votre compte Google. Pour plus de détails, voir Activer la validation en deux étapes.
- Si vous avez créé votre compte à l'aide de Continuer avec Apple, l'authentification multifactorielle est probablement déjà activée dans votre compte Apple. Si ce n'est pas le cas, pour savoir comment l'activer, consultez Authentification à deux facteurs pour un compte Apple.

- Si vous avez créé votre compte à l'aide de Continuer avec GitHub, vous pouvez activer l'authentification multifactorielle via votre GitHub compte. Pour plus de détails, consultez Configuration (GitHub) de l'authentification à deux facteurs.
- Si vous avez créé votre compte à l'aide de Continue with Amazon, vous pouvez activer l'authentification multifactorielle via votre compte Amazon. Pour plus de détails, voir Qu'est-ce que la validation en deux étapes ? .

Types de MFA disponibles pour ID de constructeur AWS

ID de constructeur AWS prend en charge les types de périphériques d'authentification multifactorielle (MFA) suivants.

FIDO2 authentificateurs

FIDO2est une norme qui inclut CTAP2 WebAuthnet est basée sur la cryptographie à clé publique. Les informations d'identification FIDO résistent au hameçonnage car elles sont uniques au site Web sur lequel elles ont été créées, par exemple. AWS

AWS prend en charge les deux formats les plus courants pour les authentificateurs FIDO : les authentificateurs intégrés et les clés de sécurité. Voir ci-dessous pour plus d'informations sur les types les plus courants d'authentificateurs FIDO.

Rubriques

- Authentificateurs intégrés
- Clés de sécurité
- Gestionnaires de mots de passe, fournisseurs de clés d'accès et autres authentificateurs FIDO

Authentificateurs intégrés

Certains appareils sont dotés d'authentificateurs intégrés, tels que TouchID activé MacBook ou un appareil photo compatible avec Windows Hello. Si votre appareil est compatible avec les protocoles FIDO, notamment WebAuthn, vous pouvez utiliser votre empreinte digitale ou votre visage comme deuxième facteur. Pour plus d'informations, consultez la section Authentification FIDO.

Clés de sécurité

Vous pouvez acheter une clé de sécurité externe FIDO2 compatible USB, BLE ou NFC. Lorsque vous êtes invité à entrer un appareil MFA, appuyez sur le capteur de la touche. YubiKey ou Feitian

fabrique des appareils compatibles. Pour une liste de toutes les clés de sécurité compatibles, consultez la section Produits certifiés FIDO.

Gestionnaires de mots de passe, fournisseurs de clés d'accès et autres authentificateurs FIDO

Plusieurs fournisseurs tiers prennent en charge l'authentification FIDO dans les applications mobiles, en tant que fonctionnalité dans les gestionnaires de mots de passe, les cartes à puce dotées d'un mode FIDO et d'autres formats. Ces appareils compatibles avec FIDO peuvent fonctionner avec IAM Identity Center, mais nous vous recommandons de tester vous-même un authentificateur FIDO avant d'activer cette option pour le MFA.

> **Note**
>
> Certains authentificateurs FIDO peuvent créer des informations d'identification FIDO détectables appelées clés d'accès. Les clés d'accès peuvent être liées à l'appareil qui les a créées, ou elles peuvent être synchronisées et sauvegardées dans un cloud. Par exemple, vous pouvez enregistrer une clé d'accès à l'aide d'Apple Touch ID sur un Macbook compatible, puis vous connecter à un site depuis un ordinateur portable Windows à l'aide de Google Chrome avec votre clé d'accès dans iCloud en suivant les instructions qui s'affichent à l'écran lors de la connexion. Pour plus d'informations sur les appareils compatibles avec les clés d'accès synchronisées et sur l'interopérabilité actuelle des clés d'accès entre les systèmes d'exploitation et les navigateurs, consultez la section Support des appareils sur passkeys.dev, une ressource gérée par l'Alliance FIDO et le World Wide Web Consortium (W3C).

Applications d'authentification

Les applications d'authentification sont des authentificateurs tiers basés sur un mot de passe à usage unique (OTP). Vous pouvez utiliser une application d'authentification installée sur votre appareil mobile ou votre tablette en tant qu'appareil MFA autorisé. L'application d'authentification tierce doit être conforme à la RFC 6238, qui est un algorithme de mot de passe à usage unique (TOTP) basé sur des normes et basé sur le temps capable de générer des codes d'authentification à six chiffres.

Lorsque vous êtes invité à saisir le MFA, vous devez saisir un code valide provenant de votre application d'authentification dans la zone de saisie qui s'affiche. Chaque dispositif MFA attribué à un utilisateur doit être unique. Deux applications d'authentification peuvent être enregistrées pour un utilisateur donné.

Vous pouvez choisir parmi les applications d'authentification tierces bien connues suivantes. Cependant, toute application compatible TOTP fonctionne avec le ID de constructeur AWS MFA.

Système d'exploitation	Application d'authentification testée
Android	1Password, Authy, Duo Mobile, Microsoft Authenticator, Google Authenticator
iOS	1Password, Authy, Duo Mobile, Microsoft Authenticator, Google Authenticator

Enregistrez votre appareil ID de constructeur AWS MFA

> **Note**
>
> Une fois que vous vous êtes inscrit à l'authentification MFA, que vous vous êtes déconnecté, puis que vous vous êtes connecté sur le même appareil, il se peut que vous ne soyez pas invité à utiliser l'authentification MFA sur les appareils approuvés.

Pour enregistrer votre appareil MFA à l'aide d'une application d'authentification

1. Connectez-vous à votre ID de constructeur AWS profil à l'adressehttps://profile.aws.amazon.com.
2. Choisissez Security (Sécurité).
3. Sur la page Sécurité, choisissez Enregistrer l'appareil.
4. Sur la page Enregistrer un appareil MFA, choisissez l'application Authenticator.
5. ID de constructeur AWS fonctionne et affiche les informations de configuration, y compris un graphique de code QR. Le graphique est une représentation de la « clé de configuration secrète » qui peut être saisie manuellement dans les applications d'authentification qui ne prennent pas en charge les codes QR.
6. Ouvrez votre application d'authentification. Pour obtenir la liste des applications, consultezApplications d'authentification.

   Si l'application d'authentification prend en charge plusieurs appareils ou comptes MFA, choisissez l'option permettant de créer un nouvel appareil ou un nouveau compte MFA.

7. Déterminez si l'application MFA prend en charge les codes QR, puis effectuez l'une des opérations suivantes sur la page Configurer votre application d'authentification :

   1. Choisissez Afficher le code QR, puis utilisez l'application pour scanner le code QR. Par exemple, vous pouvez choisir l'icône de l'appareil photo ou une option similaire à Scanner le code. Utilisez ensuite l'appareil photo de l'appareil pour scanner le code.
   2. Choisissez Afficher la clé secrète, puis entrez cette clé secrète dans votre application MFA.

   Lorsque vous aurez terminé, votre application d'authentification générera et affichera un mot de passe à usage unique.

8. Dans le champ Code d'authentification, entrez le mot de passe à usage unique qui apparaît actuellement dans votre application d'authentification. Choisissez Assign MFA (Affecter le MFA).

   > **Important**
   >
   > Envoyez votre demande immédiatement après avoir généré le code. Si vous générez le code puis attendez trop longtemps pour soumettre la demande, le dispositif MFA est correctement associé au vôtre ID de constructeur AWS, mais le dispositif MFA n'est pas synchronisé. En effet, les TOTP (Time-based One-Time Passwords ou mots de passe à usage unique à durée limitée) expirent après une courte période. Dans ce cas, vous pouvez resynchroniser le dispositif. Pour de plus amples informations, veuillez consulter Je reçois le message « Une erreur inattendue s'est produite » lorsque j'essaie de m'inscrire ou de me connecter avec une application d'authentification.

9. Pour attribuer un nom convivial à votre appareil ID de constructeur AWS, choisissez Renommer. Ce nom vous permet de distinguer cet appareil des autres appareils que vous enregistrez.

Le dispositif MFA est maintenant prêt à être utilisé avec. ID de constructeur AWS

Enregistrez une clé de sécurité en tant que ID de constructeur AWS dispositif MFA

Pour enregistrer votre appareil MFA à l'aide d'une clé de sécurité

1. Connectez-vous à votre ID de constructeur AWS profil à l'adressehttps://profile.aws.amazon.com.

2. Choisissez Security (Sécurité).
3. Sur la page Sécurité, choisissez Enregistrer l'appareil.
4. Sur la page Enregistrer un appareil MFA, sélectionnez Clé de sécurité.
5. Assurez-vous que votre clé de sécurité est activée. Si vous utilisez une clé de sécurité physique distincte, connectez-la à votre ordinateur.
6. Suivez les instructions qui s'affichent à l'écran. Votre expérience varie en fonction de votre système d'exploitation et de votre navigateur.
7. Pour attribuer un nom convivial à votre appareil ID de constructeur AWS, choisissez Renommer. Ce nom vous permet de distinguer cet appareil des autres appareils que vous enregistrez.

Le dispositif MFA est maintenant prêt à être utilisé avec. ID de constructeur AWS

Renommez votre appareil ID de constructeur AWS MFA

Pour renommer votre appareil MFA

1. Connectez-vous à votre ID de constructeur AWS profil à l'adressehttps://profile.aws.amazon.com.
2. Choisissez Security (Sécurité). Lorsque vous arrivez sur la page, vous voyez que Renommer est grisé.
3. Sélectionnez le périphérique MFA que vous souhaitez modifier. Cela vous permet de choisir Renommer. Ensuite, une boîte de dialogue apparaît.
4. Dans l'invite qui s'affiche, entrez le nouveau nom dans le champ Nom du périphérique MFA, puis choisissez Renommer. L'appareil renommé apparaît sous Appareils d'authentification multifactorielle (MFA).

Supprimer votre appareil MFA

Nous vous recommandons de conserver au moins deux appareils MFA actifs. Avant de supprimer un appareil, consultez la section Enregistrez votre appareil ID de constructeur AWS MFA pour enregistrer un appareil MFA de remplacement. Pour désactiver l'authentification multifactorielle pour vous ID de constructeur AWS, supprimez tous les appareils MFA enregistrés de votre profil.

Pour supprimer un appareil MFA

1. Connectez-vous à votre ID de constructeur AWS profil à l'adressehttps://profile.aws.amazon.com.
2. Choisissez Security (Sécurité).
3. Sélectionnez le périphérique MFA que vous souhaitez modifier, puis choisissez Supprimer.
4. Dans le dispositif Delete MFA ? modal, suivez les instructions pour supprimer votre appareil.
5. Sélectionnez Delete (Supprimer).

L'appareil supprimé n'apparaît plus sous les appareils d'authentification multifactorielle (MFA).

Confidentialité et données dans ID de constructeur AWS

La AWS déclaration de confidentialité décrit la manière dont nous traitons vos données personnelles. Pour plus d'informations sur la façon de supprimer votre ID de constructeur AWS profil, consultezSupprimez votre ID de constructeur AWS.

Demandez vos ID de constructeur AWS données

Vous pouvez demander et consulter les informations personnelles associées à vous ID de constructeur AWS et aux AWS applications et services auxquels vous avez accédé avec votre ID de constructeur AWS. Pour plus d'informations sur l'exercice de vos droits en tant que personne concernée, y compris pour les informations personnelles fournies en relation avec d'autres AWS sites Web, applications, produits, services, événements et expériences, consultezhttps://aws.amazon.com/privacy.

Pour demander vos données

1. Connectez-vous à votre ID de constructeur AWS profil à l'adressehttps://profile.aws.amazon.com.
2. Choisissez Mes ID de constructeur AWS données.
3. Sur la page Mes ID de constructeur AWS données, sous Supprimer ID de constructeur AWS, choisissez Demander vos données.
4. Un message de confirmation vert apparaît en haut de la page indiquant que nous avons reçu votre demande et que nous la traiterons dans les 30 jours.

5. Lorsque vous recevez un e-mail de notre part indiquant que la demande a été traitée, revenez à la page Confidentialité et données de votre ID de constructeur AWS profil. Cliquez sur le nouveau bouton Télécharger l'archive ZIP contenant vos données.

   Tant que votre demande de données est en attente, vous ne pourrez pas supprimer votre ID de constructeur AWS.

ID de constructeur AWS et autres AWS informations d'identification

Votre identifiant ID de constructeur AWS est distinct de tout autre identifiant Compte AWS ou identifiant de connexion. Vous pouvez utiliser le même e-mail pour votre adresse e-mail ID de constructeur AWS et pour celle de l'utilisateur root d'un Compte AWS.

Et ID de constructeur AWS :

- Vous permet d'accéder aux outils et services qui utilisent ID de constructeur AWS.
- N'a aucun impact sur les contrôles de sécurité existants, tels que les politiques et les configurations que vous avez spécifiées sur vos applications Comptes AWS ou applications.
- Ne remplace aucun utilisateur, identifiant ou compte root, IAM Identity Center ou IAM existant.
- Impossible d'obtenir les informations d'identification AWS IAM pour accéder au AWS Management Console, AWS CLI AWS SDKs, ou AWS Toolkit.

An Compte AWS est un conteneur de ressources contenant des informations de contact et de paiement. Il établit une limite de sécurité dans laquelle exploiter des AWS services facturés et mesurés, tels que S3, EC2 ou Lambda. Les titulaires de comptes peuvent se connecter Compte AWS à un AWS Management Console. Pour plus d'informations, voir Se connecter au AWS Management Console.

Quel est le ID de constructeur AWS lien avec votre identité IAM Identity Center existante

En tant que propriétaire de l'identité, vous gérez le ID de constructeur AWS. Elle n'est liée à aucune autre identité que vous pourriez avoir pour une autre organisation, telle que l'école ou le travail. Vous pouvez utiliser une identité de personnel dans IAM Identity Center pour représenter votre personnalité professionnelle et privée. ID de constructeur AWS Ces identités fonctionnent de manière indépendante.

Les utilisateurs d' AWS IAM Identity Center (successeur de AWS Single Sign-On) sont gérés par un administrateur informatique ou cloud d'entreprise, ou par l'administrateur du fournisseur d'identité de l'organisation, tel qu'Okta, Ping ou Azure. Les utilisateurs d'IAM Identity Center peuvent accéder aux ressources via plusieurs comptes dans AWS Organizations.

ID de constructeur AWS Profils multiples

Vous pouvez en créer plusieurs à condition ID de constructeur AWS que chaque identifiant utilise une adresse e-mail unique. Cependant, si vous en utilisez plusieurs, il ID de constructeur AWS peut être difficile de vous souvenir de ce ID de constructeur AWS que vous avez utilisé dans quel but. Dans la mesure du possible, nous vous recommandons d'en utiliser un seul ID de constructeur AWS pour toutes vos activités liées aux AWS outils et aux services.

Déconnectez-vous de AWS

La façon dont vous vous déconnectez de votre compte Compte AWS dépend du type d' AWS utilisateur que vous êtes. Vous pouvez être un utilisateur root du compte, un utilisateur IAM, un utilisateur dans IAM Identity Center, une identité fédérée ou un utilisateur AWS Builder ID. Si vous ne savez pas quel type d'utilisateur vous êtes, consultezDéterminez votre type d'utilisateur.

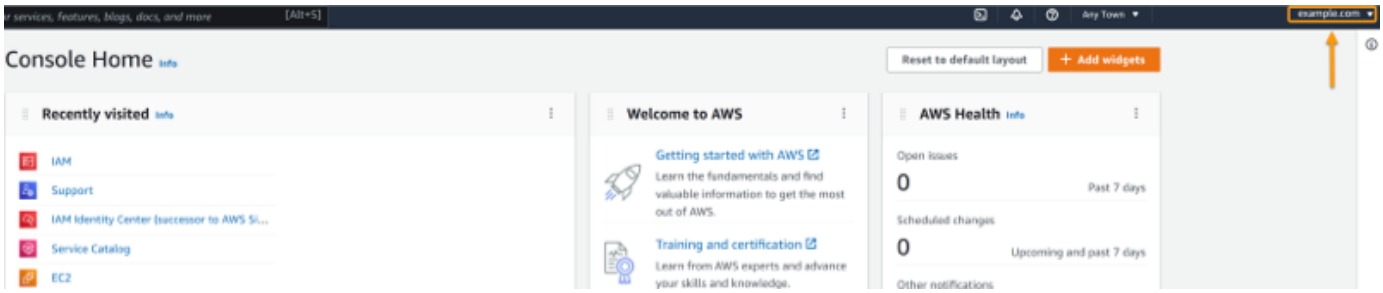
Rubriques

- Déconnectez-vous du AWS Management Console
- Déconnectez-vous de votre portail AWS d'accès
- Déconnectez-vous de AWS Builder ID

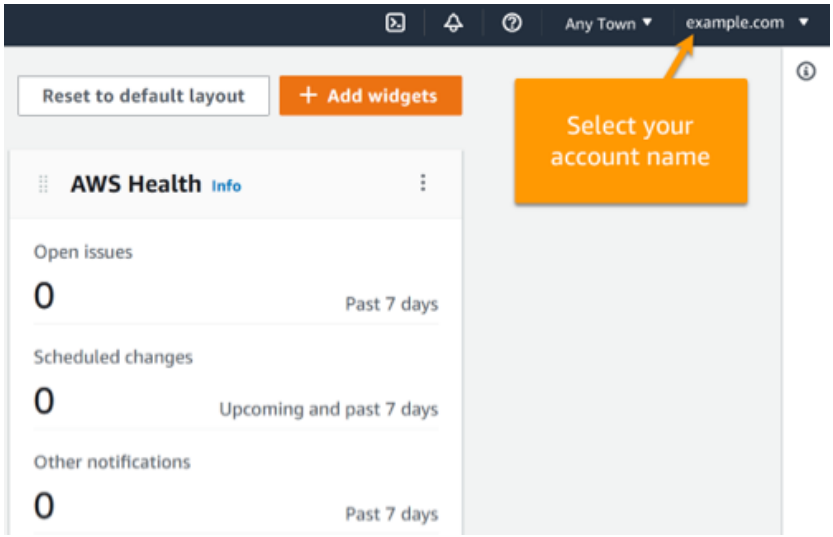
Déconnectez-vous du AWS Management Console

Pour vous déconnecter du AWS Management Console

1. Une fois connecté au AWS Management Console, vous arrivez sur une page similaire à celle illustrée dans l'image suivante. Le nom de votre compte ou nom d'utilisateur IAM est affiché dans le coin supérieur droit.



2. Dans la barre de navigation en haut à droite, choisissez votre nom d'utilisateur.



3. Choisissez une option de déconnexion. Les options des boutons varient en fonction du nombre de comptes auxquels vous êtes connecté.

   - Sélectionnez Déconnexion si vous n'êtes connecté qu'à un seul compte.
   - Sélectionnez Se déconnecter de toutes les sessions pour vous déconnecter de toutes vos identités simultanément.
   - Sélectionnez Se déconnecter de la session en cours pour vous déconnecter de l'identité que vous avez sélectionnée.

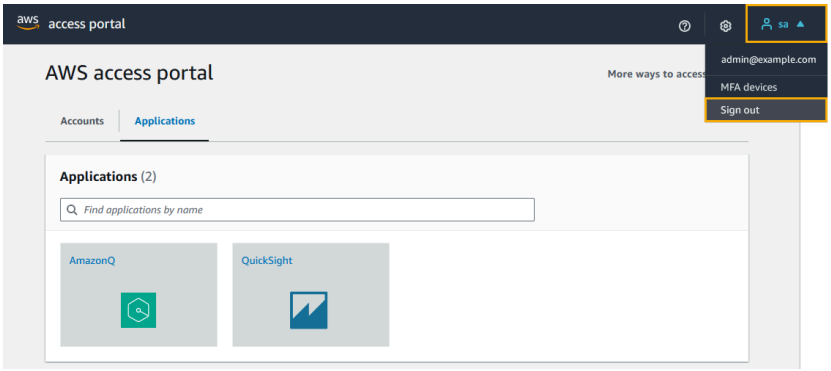
4. Vous êtes redirigé vers la AWS Management Console page Web.

Pour plus d'informations sur la connexion à plusieurs comptes, consultez la section Connexion à plusieurs comptes dans le Guide de AWS Management Console démarrage.

Déconnectez-vous de votre portail AWS d'accès

Pour vous déconnecter de votre portail AWS d'accès

1. Dans la barre de navigation en haut à droite, choisissez votre nom d'utilisateur.
2. Sélectionnez Se déconnecter comme indiqué dans l'image suivante.



3. Si vous vous déconnectez avec succès, la page de connexion de votre portail AWS d'accès s'affiche désormais.

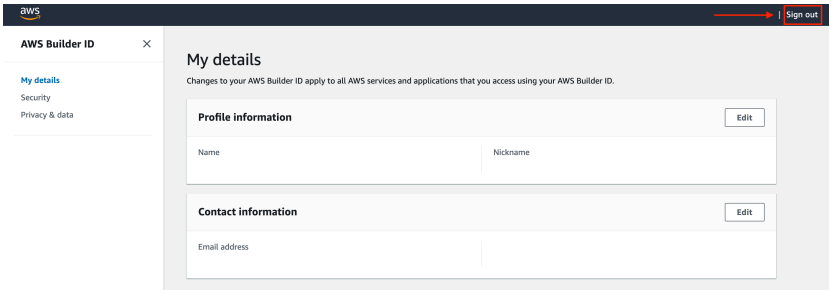
Si vous utilisez un fournisseur d'identité externe (IdP) comme source d'identité, la session active pour vos informations d'identification n'est pas interrompue lorsque vous vous déconnectez. Si vous revenez au portail AWS d'accès, il se peut que vous soyez automatiquement connecté sans avoir à fournir vos informations d'identification.

Déconnectez-vous de AWS Builder ID

Pour vous déconnecter d'un AWS service auquel vous avez accédé à l'aide de votre identifiant AWS Builder, vous devez vous déconnecter du service. Si vous souhaitez vous déconnecter de votre profil AWS Builder ID, consultez la procédure suivante.

Pour vous déconnecter de votre profil AWS Builder ID

1. Après vous être connecté à votre profil AWS Builder ID à l'https://profile.aws.amazon.com/adresse, vous accédez à Mes coordonnées.
2. Dans le coin supérieur droit de votre page de profil AWS Builder ID, choisissez Se déconnecter.



3. Vous êtes déconnecté lorsque vous ne voyez plus votre profil AWS Builder ID.

Résolution des problèmes Compte AWS problèmes de connexion

Utilisez les informations fournies ici pour vous aider à résoudre les problèmes de connexion et autres Compte AWS . Pour obtenir des instructions détaillées sur la connexion à un Compte AWS, voirConnectez-vous au AWS Management Console.

Si aucune des rubriques de résolution des problèmes ne vous aide à résoudre votre problème de connexion, vous pouvez créer un dossier Support en remplissant ce formulaire : Je suis AWS client et je recherche une assistance concernant la facturation ou le compte. En matière de sécurité, il est recommandé de Support ne pas discuter des détails d'un compte Compte AWS autre que le compte auquel vous êtes connecté. AWS Support ne peut pas non plus modifier les informations d'identification associées à un compte pour quelque raison que ce soit.

> **Note**
>
> Support ne publie pas de numéro de téléphone direct permettant de joindre un représentant du support.

Pour obtenir de l'aide sur la résolution de vos problèmes de connexion, consultez Que dois-je faire si je ne parviens pas à me connecter ou à accéder à mon Compte AWS ? Si vous ne parvenez pas à vous connecter Amazon.com, contactez le service client Amazon au lieu de cette page.

Rubriques

- Comment puis-je trouver mon Compte AWS ID ou alias
- J'ai besoin du code de vérification de mon compte
- J'ai oublié le mot de passe de mon utilisateur root pour mon Compte AWS
- J'ai oublié mon mot de passe utilisateur IAM pour mon Compte AWS
- J'ai oublié le mot de passe d'identité fédérée pour mon Compte AWS
- Je n'arrive pas à me connecter à mon compte existant Compte AWS et je n'arrive pas à créer un nouveau Compte AWS avec la même adresse e-mail
- Je dois réactiver mon appareil suspendu Compte AWS
- J'ai besoin de contacter Support pour les problèmes de connexion
- J'ai besoin de contacter AWS Billing pour des problèmes de facturation
- J'ai une question concernant une commande au détail
- J'ai besoin d'aide pour gérer mon Compte AWS
- Mon AWS les informations d'identification du portail d'accès ne fonctionnent pas
- J'ai oublié le mot de passe IAM Identity Center pour mon Compte AWS
- Je reçois un message d'erreur indiquant « Ce n'est pas vous, c'est nous » lorsque j'essaie de me connecter à la console IAM Identity Center

Mon AWS Management Console les informations d'identification ne fonctionnent pas

Si vous vous souvenez de votre nom d'utilisateur et de votre mot de passe, mais que vos informations d'identification ne fonctionnent pas, vous êtes peut-être sur la mauvaise page. Essayez de vous connecter sur une autre page :

Page de connexion d'utilisateur racine

- Si vous avez créé ou possédez un compte Compte AWS et que vous effectuez une tâche qui nécessite des informations d'identification d'utilisateur root, entrez l'adresse e-mail de votre compte dans le AWS Management Console. Pour savoir comment accéder à l'utilisateur root, consultezPour vous connecter en tant qu'utilisateur root. Si vous avez oublié le mot de passe de votre utilisateur root, vous pouvez le réinitialiser. Pour plus d'informations, consultez J'ai oublié le mot de passe de mon utilisateur root pour mon Compte AWS. Si vous avez oublié l'adresse e-mail de votre utilisateur root, consultez votre boîte de réception pour y trouver un e-mail provenant de AWS.

- Si vous avez essayé de vous connecter à votre compte utilisateur root et que vous avez reçu le message d'erreur suivant : La récupération du mot de passe est désactivée pour mon compte utilisateur root, vous n'avez aucun identifiant d'utilisateur root. Vous ne pouvez pas vous connecter en tant qu'utilisateur root ni récupérer le mot de passe de l'utilisateur root de votre compte. AWS les comptes membres gérés via AWS Organizations peuvent ne pas avoir de mot de passe utilisateur root, de clés d'accès, de certificats de signature ou d'authentification multifactorielle (MFA) active.

  Seul le compte de gestion ou l'administrateur délégué d'IAM peut effectuer des actions d'utilisateur root sur votre compte membre. Contactez votre administrateur si vous devez effectuer une tâche qui nécessite les informations d'identification de l'utilisateur racine. Pour plus d'informations, voir Gestion centralisée de l'accès root pour les comptes des membres dans le Guide de Gestion des identités et des accès AWS l'utilisateur.

Page de connexion utilisateur IAM

- Si vous ou quelqu'un d'autre avez créé un utilisateur IAM dans un Compte AWS, vous devez connaître cet Compte AWS identifiant ou cet alias pour vous connecter. Entrez votre identifiant ou alias de compte, votre nom d'utilisateur et votre mot de passe dans le AWS Management Console. Pour savoir comment accéder à la page de connexion utilisateur IAM, consultez. Pour vous connecter en tant qu'utilisateur IAM Si vous avez oublié votre mot de passe utilisateur IAM, vous pouvez consulter des informations sur J'ai oublié mon mot de passe utilisateur IAM pour mon Compte AWS la réinitialisation de votre mot de passe utilisateur IAM. Si vous avez oublié votre numéro de compte, recherchez dans votre e-mail, les favoris ou l'historique de votre navigateur une URL contenant `signin.aws.amazon.com/`. Votre identifiant ou alias de compte suivra le texte `"account="` dans l'URL. Si vous ne trouvez pas votre identifiant de compte ou votre alias, contactez votre administrateur. Support Je ne peux pas vous aider à récupérer ces informations. Vous ne pouvez voir votre identifiant ou alias de compte qu'après vous être connecté.

La réinitialisation du mot de passe est requise pour mon utilisateur root

Pour protéger votre compte, vous pouvez recevoir le message suivant lorsque vous essayez de vous connecter au AWS Management Console :

La réinitialisation du mot de passe est requise. Pour des raisons de sécurité, vous devez réinitialiser votre mot de passe. Pour garantir la sécurité de votre compte, vous devez sélectionner Mot de passe oublié ci-dessous et réinitialiser votre mot de passe.

En plus de ce message, il vous avertit AWS également lorsque nous identifions un problème potentiel par le biais de l'e-mail associé à votre compte. Cet e-mail indique la raison pour laquelle la réinitialisation du mot de passe est requise. Par exemple, lorsque nous détectons une activité de connexion inhabituelle Compte AWS ou que les informations d'identification qui vous Compte AWS sont associées sont accessibles au public en ligne.

Mettez à jour votre mot de passe pour garantir la sécurité de vos informations d'identification d'utilisateur root. Pour savoir comment réinitialiser le mot de passe de votre utilisateur root, voir J'ai oublié mon mot de passe utilisateur root pour mon compte Compte AWS.

Je n'ai pas accès à l'e-mail de mon Compte AWS

Lorsque vous créez un Compte AWS, vous fournissez une adresse e-mail et un mot de passe. Ce sont les informations d'identification pour le Utilisateur racine d'un compte AWS. Si vous n'êtes pas sûr de l'adresse e-mail associée à votre compte Compte AWS, recherchez la correspondance enregistrée se terminant par @signin .aws ou @verify .signin.aws et renvoyant à n'importe quelle adresse e-mail de votre organisation qui aurait pu être utilisée pour ouvrir le. Compte AWS Demandez aux autres membres de votre équipe, de votre organisation ou de votre famille. Si quelqu'un que vous connaissez a créé le compte, il peut vous aider à y accéder.

Si vous connaissez l'adresse e-mail, mais que vous n'avez plus accès à l'e-mail, essayez d'abord de récupérer l'accès à l'e-mail en utilisant l'une des options suivantes :

- Si vous possédez le domaine pour l'adresse e-mail, vous pouvez restaurer une adresse e-mail supprimée. Vous pouvez également configurer un « catch-all » pour votre compte de messagerie, qui « attrape tous » les messages envoyés à des adresses e-mail qui n'existent plus dans le serveur de messagerie et les redirige vers une autre adresse e-mail.
- Si l'adresse e-mail sur le compte fait partie de votre système de messagerie d'entreprise, nous vous recommandons de contacter vos administrateurs de système informatique. Ils peuvent vous aider à récupérer l'accès à l'e-mail.

Si vous ne parvenez toujours pas à vous connecter à votre Compte AWS, vous pouvez trouver d'autres options d'assistance en contactant Support.

Mon appareil MFA est perdu ou ne fonctionne plus

Si votre appareil MFA est perdu, endommagé ou ne fonctionne pas, vous ne recevez pas de code à usage unique (OTP) lorsque vous envoyez une demande de vérification MFA.

Utilisateurs IAM

Vous pouvez vous connecter à l'aide d'un autre appareil MFA enregistré auprès du même utilisateur IAM.

Les utilisateurs IAM doivent contacter un administrateur pour désactiver un dispositif MFA qui ne fonctionne pas. Ces utilisateurs ne peuvent pas récupérer leur appareil MFA sans l'assistance de l'administrateur. Votre administrateur est généralement un membre du personnel des technologies de l'information (IT) qui dispose d'un niveau d'autorisations supérieur à Compte AWS celui des autres membres de votre organisation. Cette personne a créé votre compte et fournit aux utilisateurs leurs identifiants d'accès pour se connecter.

Utilisateurs root

Pour récupérer l'accès à l'utilisateur root, vous devez vous connecter à l'aide d'un autre périphérique MFA enregistré auprès du même utilisateur root. Passez ensuite en revue les options suivantes pour récupérer ou mettre à jour votre appareil MFA :

- Pour obtenir des instructions détaillées pour récupérer un appareil MFA, voir Que faire si un appareil MFA est perdu ou cesse de fonctionner ?
- Pour obtenir des instructions détaillées sur la façon de mettre à jour le numéro de téléphone d'un appareil MFA, voir Comment mettre à jour mon numéro de téléphone pour réinitialiser mon appareil MFA perdu ?
- Pour obtenir des instructions détaillées sur l'activation des appareils MFA, consultez la section Activation des appareils MFA pour les utilisateurs dans. AWS
- Si vous ne parvenez pas à récupérer votre appareil MFA, contactez. Support

> **Note**
>
> Les utilisateurs IAM doivent contacter leur administrateur pour obtenir de l'aide concernant les appareils MFA. Support ne peut pas aider les utilisateurs IAM à résoudre des problèmes liés aux appareils MFA.

Je ne parviens pas à accéder au AWS Management Console page de connexion

Si vous ne pouvez pas voir votre page de connexion, le domaine est peut-être bloqué par un pare-feu. Contactez votre administrateur réseau pour ajouter les domaines ou points de terminaison d'URL suivants aux listes autorisées de votre solution de filtrage de contenu Web en fonction du type d'utilisateur que vous êtes et de la manière dont vous vous connectez.

Utilisateur root et utilisateurs IAM	*.signin.aws.amazon.com
Amazon.com connexion au compte	www.amazon.com
Utilisateurs d'IAM Identity Center et connexion à une application propriétaire	• *.awsapps.com () http://awsapps.com/ • *.signin.aws

Je ne peux pas me connecter en raison de l'état du réseau dans les politiques basées sur les Sign-in ressources

Si l'un des messages d'erreur suivants s'affiche, une politique Sign-in basée sur les ressources ou une politique de contrôle des ressources (RCP) restreint peut-être l'accès en fonction de l'emplacement de votre réseau :

- « Vos informations d'authentification sont incorrectes. Veuillez réessayer. »
- « Échec de l'authentification Demande non valide »
- « Échec de l'authentification : pour accéder à ce compte, connectez-vous depuis un autre réseau ou contactez votre administrateur pour plus d'informations »

Contactez votre administrateur ou consultez les étapes Je ne peux pas me connecter en raison de l'état du réseau dans les politiques basées sur les Sign-in ressources de résolution des problèmes détaillées.

L'accès à mon compte est bloqué après avoir activé l'autorisation de la console

Si vous avez configuré l'autorisation de console et que vous ne pouvez plus accéder à votre compte, il se peut que vous n'ayez pas configuré les principaux exclus ou l'accès de restauration d'urgence avant d'appliquer la politique. Pour les étapes de résolution, y compris le libre-service de la AWS CLI`OrganizationAccountAccessRole`, les options et AWS Support, consultezL'accès à mon compte est bloqué après avoir activé l'autorisation de la console.

Les modifications de ma politique ne prennent pas effet

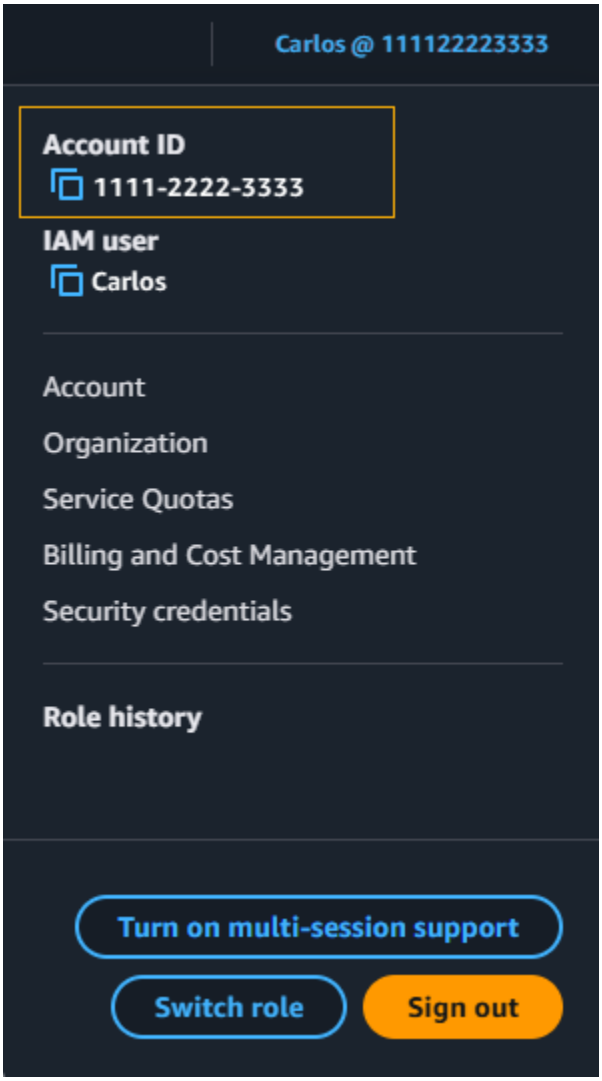
Les modifications apportées à la configuration des autorisations de console et aux instructions d'autorisation des ressources sont répliquées globalement et peuvent prendre quelques minutes pour prendre effet. Si vos modifications ne sont pas visibles après avoir attendu, consultez Les modifications que j'apporte ne sont pas toujours visibles immédiatement les étapes de résolution des problèmes.

Comment puis-je trouver mon Compte AWS ID ou alias

Si vous êtes un utilisateur IAM et que vous n'êtes pas connecté, demandez l' Compte AWS ID ou l'alias à votre administrateur. Votre administrateur est généralement un membre du personnel des technologies de l'information (IT) qui dispose d'un niveau d'autorisations supérieur à Compte AWS celui des autres membres de votre organisation. Cette personne a créé votre compte et fournit aux utilisateurs leurs identifiants d'accès pour se connecter.

Si vous êtes un utilisateur IAM ayant accès au AWS Management Console, votre identifiant de compte se trouve dans votre URL de connexion. Consultez les e-mails de votre administrateur pour connaître l'URL de connexion. L'identifiant du compte est constitué des douze premiers chiffres de l'URL de connexion. Par exemple, dans l'URL suivante`https://111122223333.signin.aws.amazon.com/console`, votre Compte AWS identifiant est 111122223333.

Une fois connecté au AWS Management Console, vous trouverez les informations de votre compte dans la barre de navigation à côté de votre région. Par exemple, dans la capture d'écran suivante, l'utilisateur IAM Carlos possède le numéro Compte AWS 1111-2222-3333.



Pour plus d'informations sur votre Compte AWS identifiant et votre alias et sur la façon de les trouver, consultez la section Votre Compte AWS identifiant et son alias.

J'ai besoin du code de vérification de mon compte

Si vous avez fourni l'adresse e-mail et le mot de passe de votre compte, AWS il vous est parfois demandé de fournir un code de vérification à usage unique. Pour récupérer le code de vérification, vérifiez que l'e-mail qui vous est associé Compte AWS contient un message provenant d'Amazon Web Services. L'adresse e-mail se termine par @signin .aws ou @verify .signin.aws. Suivez les instructions du message. Si le message n'apparaît pas dans votre compte, vérifiez vos dossiers de courrier indésirable et de courrier indésirable. Si vous n'avez plus accès à l'adresse e-mail, consultez Je n'ai pas accès à l'e-mail de mon Compte AWS.

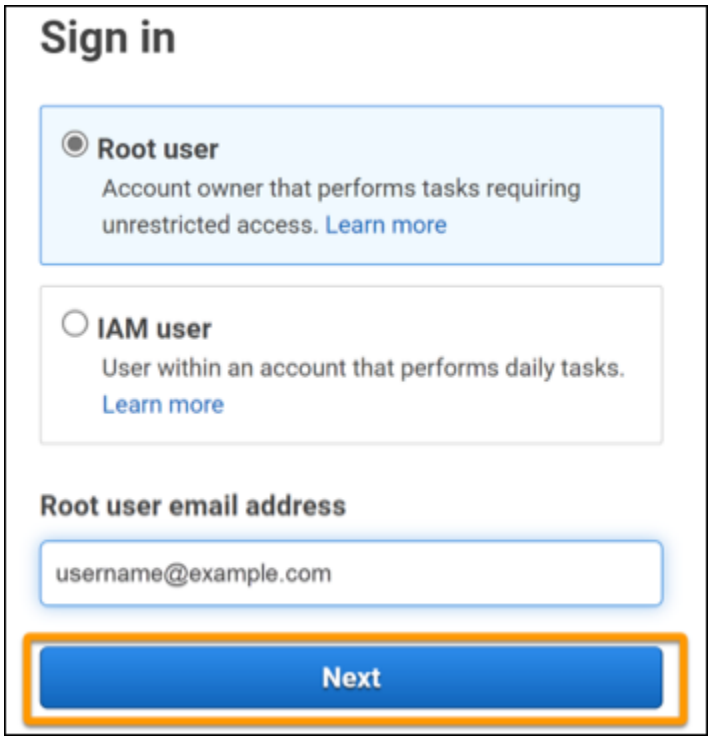
J'ai oublié le mot de passe de mon utilisateur root pour mon Compte AWS

Si vous êtes un utilisateur root et que vous avez perdu ou oublié le mot de passe de votre Compte AWS compte, vous pouvez le réinitialiser en sélectionnant le lien « Mot de passe oublié » dans le AWS Management Console. Vous devez connaître l'adresse e-mail de votre AWS compte et y avoir accès. Un lien vous sera envoyé par e-mail pendant le processus de récupération du mot de passe pour réinitialiser votre mot de passe. Le lien sera envoyé à l'adresse e-mail que vous avez utilisée pour créer votre Compte AWS.

Pour réinitialiser le mot de passe d'un compte que vous avez créé à l'aide d' AWS Organizations, consultez la section Accès à un compte membre en tant qu'utilisateur root.

Pour réinitialiser votre mot de passe utilisateur racine

1. Utilisez votre adresse AWS e-mail pour commencer à vous connecter à la console AWS de gestion en tant qu'utilisateur root. Ensuite, choisissez Suivant.

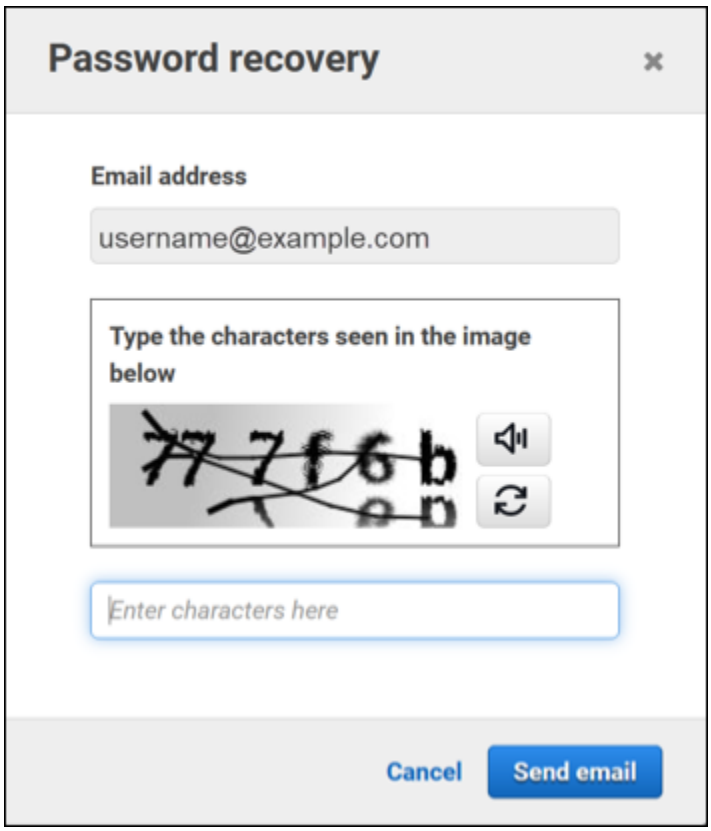


> **Note**
>
> Si vous êtes connecté à l'AWS Management Consoleaide des informations d'identification utilisateur IAM, vous devez vous déconnecter avant de pouvoir réinitialiser

le mot de passe de l'utilisateur root. Si vous voyez la page de connexion utilisateur IAM spécifique au compte, choisissez d'Sign-in utiliser les informations d'identification du compte root en bas de la page. Si nécessaire, fournissez l'adresse e-mail de votre compte et choisissez Next (Suivant) pour accéder à la page Root user sign in (Connexion de l'utilisateur racine).

2. Choisissez Mot de passe oublié ?

3. Effectuez les étapes de récupération du mot de passe. Si vous ne parvenez pas à terminer le contrôle de sécurité, essayez d'écouter le son ou d'actualiser le contrôle de sécurité pour y ajouter un nouveau jeu de caractères. Un exemple de page de récupération de mot de passe est illustré dans l'image suivante.

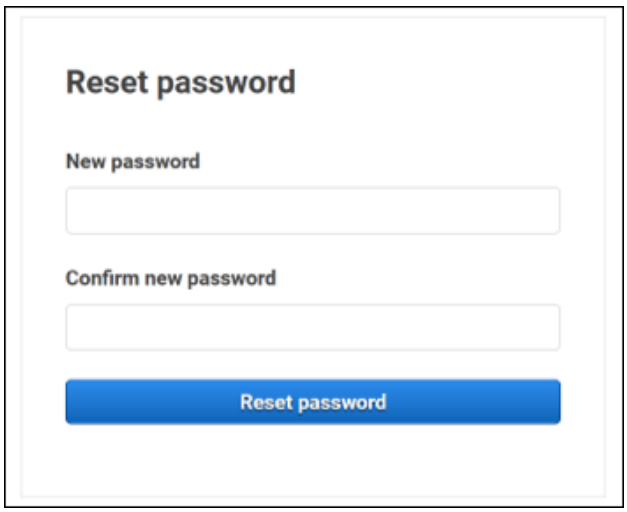


4. Après avoir terminé les étapes de récupération du mot de passe, vous recevez un message indiquant que des instructions supplémentaires ont été envoyées à l'adresse e-mail associée à votre Compte AWS.

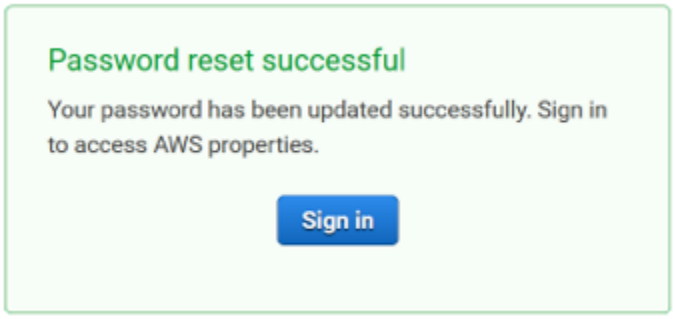
   Un e-mail contenant un lien pour réinitialiser votre mot de passe est envoyé à l'adresse e-mail utilisée pour créer le Compte AWS.

   > **Note**
   >
   > L'e-mail proviendra d'une adresse se terminant par @signin .aws ou @verify .signin.aws.

5. Sélectionnez le lien fourni dans l' AWS e-mail pour réinitialiser votre mot de passe utilisateur AWS root.
6. Le lien vous dirige vers une nouvelle page Web pour créer un nouveau mot de passe utilisateur root.



Vous recevez une confirmation indiquant que la réinitialisation de votre mot de passe a été effectuée avec succès. Une réinitialisation réussie du mot de passe est illustrée dans l'image suivante.



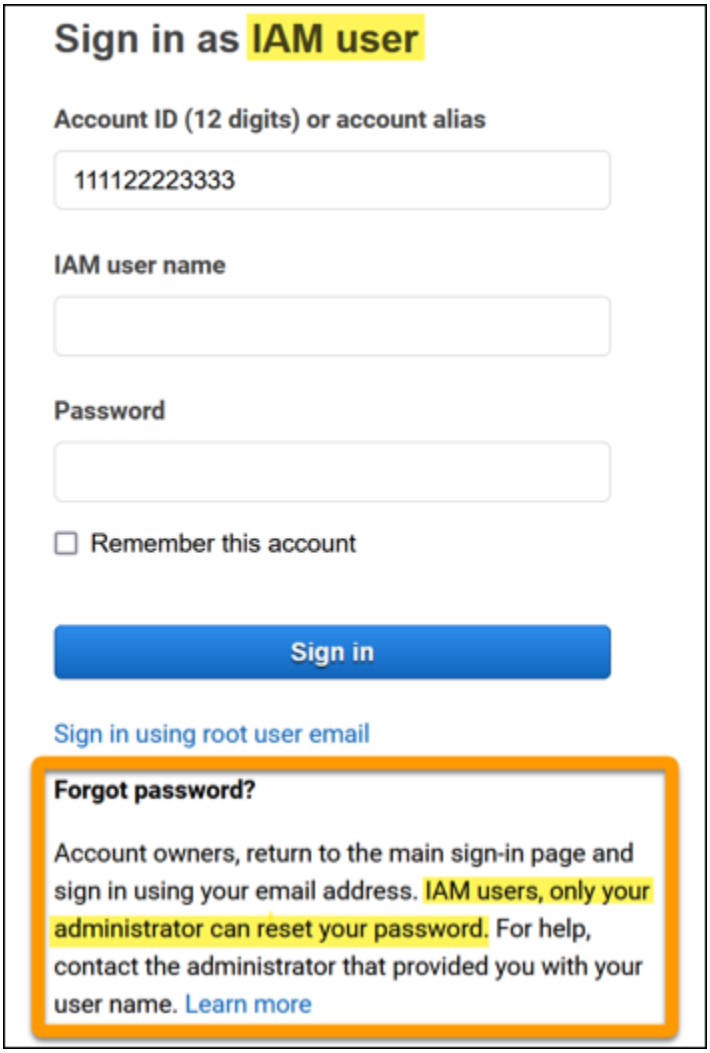
Pour plus d'informations sur la réinitialisation de votre mot de passe utilisateur root, consultez Comment récupérer un mot de AWS passe perdu ou oublié ?

J'ai oublié mon mot de passe utilisateur IAM pour mon Compte AWS

Pour modifier votre mot de passe utilisateur IAM, vous devez disposer des autorisations appropriées. Pour plus d'informations sur la réinitialisation de votre mot de passe utilisateur IAM, consultez Comment un utilisateur IAM modifie son propre mot de passe.

Si vous n'êtes pas autorisé à réinitialiser votre mot de passe, seul votre administrateur IAM peut réinitialiser le mot de passe utilisateur IAM. Les utilisateurs IAM doivent contacter leur administrateur IAM pour réinitialiser leur mot de passe. Votre administrateur est généralement un membre du

personnel des technologies de l'information (IT) qui dispose d'un niveau d'autorisations supérieur à Compte AWS celui des autres membres de votre organisation. Cette personne a créé votre compte et fournit aux utilisateurs leurs identifiants d'accès pour se connecter.



Pour des raisons de sécurité, Support n'est pas autorisé à consulter, fournir ou modifier vos informations d'identification.

Pour plus d'informations sur la réinitialisation de votre mot de passe utilisateur IAM, consultez Comment récupérer un mot de passe perdu ou oublié AWS ?

Pour savoir comment un administrateur peut gérer votre mot de passe, consultez la section Gestion des mots de passe pour les utilisateurs IAM.

J'ai oublié le mot de passe d'identité fédérée pour mon Compte AWS

Les identités fédérées se connectent pour accéder Comptes AWS avec des identités externes. Le type d'identité externe utilisé détermine la manière dont les identités fédérées se connectent. Votre administrateur crée des identités fédérées. Consultez votre administrateur pour plus de détails sur la façon de réinitialiser votre mot de passe. Votre administrateur est généralement un membre du personnel des technologies de l'information (IT) qui dispose d'un niveau d'autorisations supérieur à Compte AWS celui des autres membres de votre organisation. Cette personne a créé votre compte et fournit aux utilisateurs leurs identifiants d'accès pour se connecter.

Je n'arrive pas à me connecter à mon compte existant Compte AWS et je n'arrive pas à créer un nouveau Compte AWS avec la même adresse e-mail

Vous ne pouvez associer une adresse e-mail qu'à une seule adresse Utilisateur racine d'un compte AWS. Si vous fermez votre compte utilisateur root et qu'il reste fermé pendant plus de 90 jours, vous ne pourrez pas le rouvrir ou en créer un nouveau à Compte AWS l'aide de l'adresse e-mail associée à ce compte.

Pour résoudre ce problème, vous pouvez utiliser le sous-adressage dans lequel vous ajoutez un signe plus (+) après votre adresse e-mail habituelle lorsque vous créez un nouveau compte. Le signe plus (+) peut être suivi de lettres majuscules ou minuscules, de chiffres ou d'autres caractères compatibles avec le protocole SMTP (Simple Mail Transfer Protocol). Par exemple, vous pouvez utiliser `email+1@yourcompany.com` ou `email+tag@yourcompany.com` là où se trouve votre adresse e-mail habituelle`email@yourcompany.com`. Cette adresse est considérée comme une nouvelle adresse même si elle est connectée à la même boîte de réception que votre adresse e-mail habituelle. Avant de créer un nouveau compte, nous vous recommandons d'envoyer un e-mail test à l'adresse e-mail que vous avez ajoutée pour confirmer que votre fournisseur de messagerie prend en charge le sous-adressage.

Je dois réactiver mon appareil suspendu Compte AWS

Si votre Compte AWS compte est suspendu et que vous souhaitez le rétablir, consultez Comment puis-je réactiver mon compte suspendu ? Compte AWS

J'ai besoin de contacter Support pour les problèmes de connexion

Si vous avez tout essayé, vous pouvez obtenir de l'aide Support en remplissant la demande de Support relatif à la facturation et au compte.

J'ai besoin de contacter AWS Billing pour des problèmes de facturation

Si vous ne parvenez pas à vous connecter à votre compte Compte AWS et que vous souhaitez nous contacter AWS Billing pour des problèmes de facturation, vous pouvez le faire par le biais d'une demande de Support relatif à la facturation et aux comptes. Pour plus d'informations AWS Billing and Cost Management, notamment sur vos frais et vos modes de paiement, consultez Obtenir de l'aide en matière de AWS Billing.

J'ai une question concernant une commande au détail

Si vous rencontrez un problème avec votre compte www.amazon.com ou si vous avez une question concernant une commande au détail, consultez la section Options de support et contactez-nous.

J'ai besoin d'aide pour gérer mon Compte AWS

Si vous avez besoin d'aide pour modifier votre carte de crédit Compte AWS, signaler une activité frauduleuse ou fermer votre compte Compte AWS, consultez la section Résolution d'autres problèmes liés à Comptes AWS.

Mon AWS les informations d'identification du portail d'accès ne fonctionnent pas

Lorsque vous ne parvenez pas à vous connecter à votre portail AWS d'accès, essayez de vous souvenir de la manière dont vous y avez accédé précédemment AWS.

Si vous ne vous souvenez pas du tout d'avoir utilisé un mot de passe

Vous y avez peut-être déjà accédé AWS sans utiliser AWS d'informations d'identification. Cela est courant pour l'authentification unique professionnelle via IAM Identity Center. L'accès de AWS cette

manière signifie que vous utilisez les informations d'identification de votre entreprise pour accéder à AWS des comptes ou à des applications sans avoir à saisir vos informations d'identification.

- AWS portail d'accès : si un administrateur vous autorise à utiliser des informations d'identification externes AWS pour accéder AWS, vous avez besoin de l'URL de votre portail. Consultez votre e-mail, les favoris ou l'historique de votre navigateur pour trouver une URL qui inclut `awsapps.com/start` ou `signin.aws/platform/login`.

  Par exemple, votre URL personnalisée peut inclure un identifiant ou un domaine tel que `https://d-1234567890.awsapps.com/start`. Si vous ne trouvez pas le lien vers votre portail, contactez votre administrateur. Support Je ne peux pas vous aider à récupérer ces informations.

Si vous vous souvenez de votre nom d'utilisateur et de votre mot de passe, mais que vos informations d'identification ne fonctionnent pas, vous êtes peut-être sur la mauvaise page. Examinez l'URL dans votre navigateur Web, s'il s'agit d'un utilisateur fédéré ou d'un utilisateur d'IAM Identity Center qui ne peut pas se connecter à l'aide de ses informations d'identification. https://signin.aws.amazon.com/

- AWS portail d'accès : si un administrateur a configuré une source d'identité AWS IAM Identity Center (successeur de AWS Single Sign-On) pour AWS, vous devez vous connecter à l'aide de votre nom d'utilisateur et de votre mot de passe sur le portail AWS d'accès de votre organisation. Pour trouver l'URL de votre portail, consultez vos e-mails, le stockage sécurisé des mots de passe, les favoris du navigateur ou l'historique du navigateur pour trouver une URL contenant `awsapps.com/start` ou`signin.aws/platform/login`. Par exemple, votre URL personnalisée peut inclure un identifiant ou un domaine, par exemple `https://d-1234567890.awsapps.com/start.` si vous ne trouvez pas le lien vers votre portail, contactez votre administrateur. Support Je ne peux pas vous aider à récupérer ces informations.

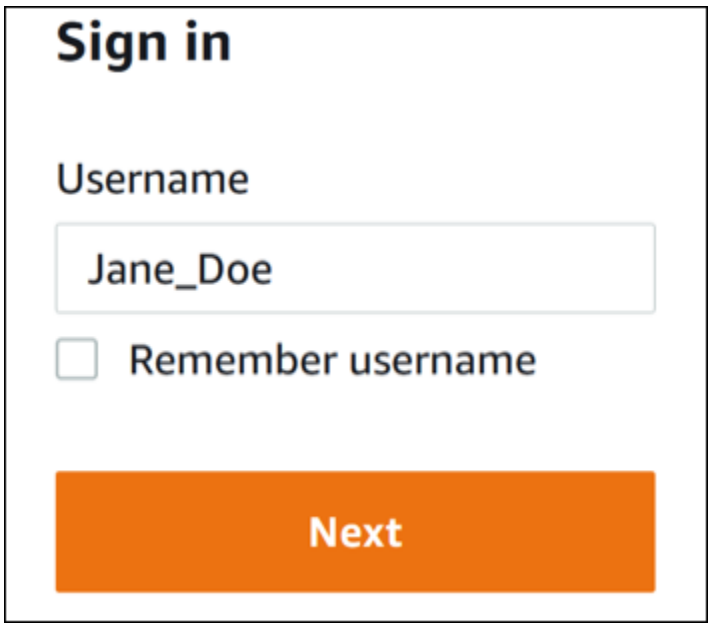
J'ai oublié le mot de passe IAM Identity Center pour mon Compte AWS

Si vous êtes un utilisateur d'IAM Identity Center et que vous avez perdu ou oublié son mot de passe Compte AWS, vous pouvez le réinitialiser. Vous devez connaître l'adresse e-mail utilisée pour le

compte IAM Identity Center et y avoir accès. Un lien pour réinitialiser votre mot de passe vous est envoyé Compte AWS par e-mail.

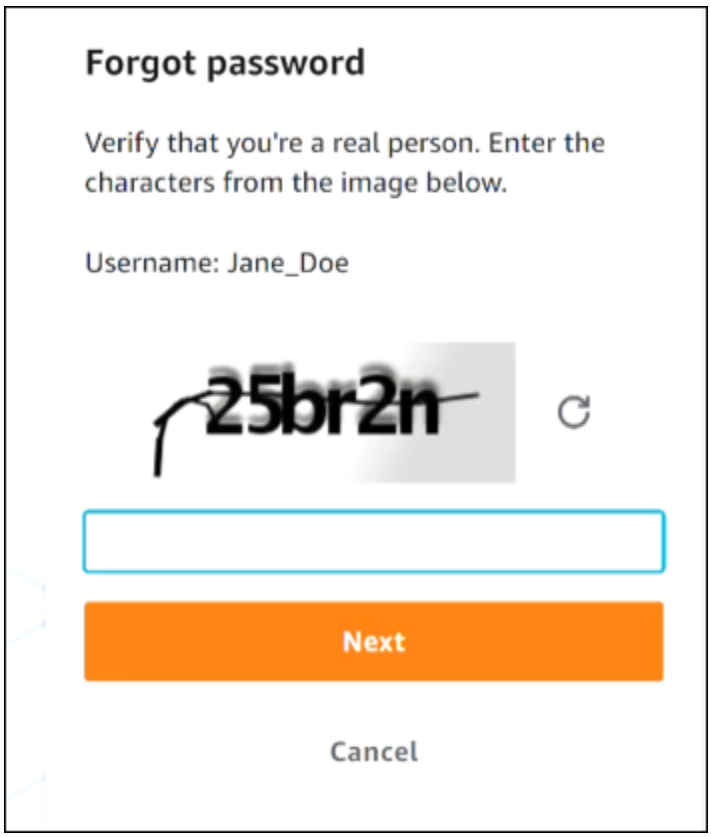
Pour réinitialiser le mot de passe de votre utilisateur dans IAM Identity Center

1. Utilisez le lien URL de votre portail d' AWS accès et entrez votre nom d'utilisateur. Ensuite, choisissez Suivant.

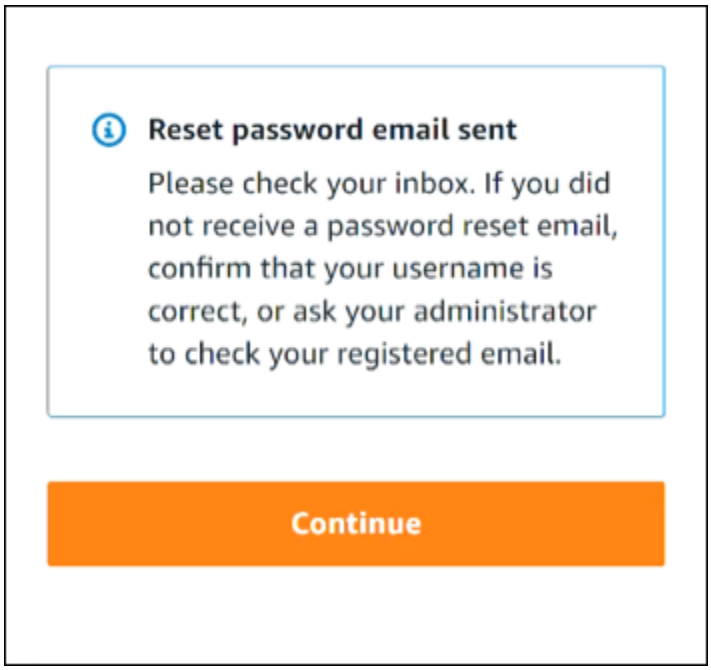


2. Sélectionnez Mot de passe oublié comme indiqué dans l'image suivante.

3. Effectuez les étapes de récupération du mot de passe.



4. Après avoir terminé les étapes de récupération du mot de passe, vous recevez le message suivant confirmant que vous avez reçu un e-mail que vous pouvez utiliser pour réinitialiser votre mot de passe.



Un e-mail contenant un lien pour réinitialiser votre mot de passe est envoyé à l'adresse e-mail associée au compte utilisateur IAM Identity Center. Sélectionnez le lien fourni dans l' AWS e-mail pour réinitialiser votre mot de passe. Le lien vous dirige vers une nouvelle page Web pour créer un nouveau mot de passe. Après avoir créé un nouveau mot de passe, vous recevez la confirmation que la réinitialisation du mot de passe a été réussie.

Si vous n'avez pas reçu d'e-mail pour réinitialiser votre mot de passe, demandez à votre administrateur de confirmer quel e-mail est enregistré auprès de votre utilisateur dans IAM Identity Center.

Je reçois un message d'erreur indiquant « Ce n'est pas vous, c'est nous » lorsque j'essaie de me connecter à la console IAM Identity Center

Cette erreur indique qu'il existe un problème de configuration avec votre instance d'IAM Identity Center ou avec le fournisseur d'identité externe (IdP) qu'elle utilise comme source d'identité. Nous vous recommandons de vérifier les points suivants :

- Vérifiez les paramètres de date et d'heure sur l'appareil que vous utilisez pour vous connecter. Nous vous recommandons d'autoriser le réglage automatique de la date et de l'heure. Si ce n'est pas le cas, nous vous recommandons de synchroniser la date et l'heure avec un serveur NTP (Network Time Protocol) connu.
- Vérifiez que le certificat IdP téléchargé vers IAM Identity Center est le même que celui fourni par votre fournisseur d'identité. Vous pouvez vérifier le certificat depuis la console IAM Identity Center en accédant aux paramètres. Dans l'onglet Source d'identité, sous Action, choisissez Gérer l'authentification. Il se peut que vous deviez importer un nouveau certificat.
- Dans le fichier de métadonnées SAML de votre IdP, assurez-vous que le format NameID est. `urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress`
- Si vous utilisez AD Connector, vérifiez que les informations d'identification du compte de service sont correctes et qu'elles n'ont pas expiré. Pour plus d'informations, consultez Mettre à jour les informations d'identification de votre compte de service AD Connector dans Directory Service.

Résolution des problèmes liés à AWS Builder ID

Utilisez les informations fournies ici pour vous aider à résoudre les problèmes que vous pourriez rencontrer avec votre ID de constructeur AWS.

Rubriques

- Je reçois le message « Ce n'est pas toi, c'est nous » lorsque j'essaie de me connecter à AWS Builder ID
- Me déconnecter ne me déconnecte pas complètement
- Je cherche toujours à résoudre mon problème

Mon adresse e-mail est déjà utilisée

Si l'e-mail que vous avez saisi est déjà utilisé et que vous le reconnaissez comme étant le vôtre, vous vous êtes peut-être déjà inscrit pour obtenir un AWS Builder ID. Essayez de vous connecter à l'aide de cette adresse e-mail. Si vous ne vous souvenez pas de votre mot de passe, consultezJ'ai oublié mon mot de passe.

Je n'arrive pas à terminer la vérification par e-mail

Si vous vous êtes inscrit à AWS Builder ID mais que vous n'avez pas reçu votre e-mail de vérification, effectuez les tâches de résolution des problèmes suivantes.

1. Vérifiez votre dossier de spam, de courrier indésirable et d'éléments supprimés.

   > **Note**
   >
   > Cet e-mail de vérification provient de l'adresse no-reply@signin.aws ou no-reply@login.awsapps.com. Nous vous recommandons de configurer votre système de messagerie de manière à ce qu'il accepte les e-mails provenant de ces adresses d'expéditeur et qu'il ne les traite pas comme du courrier indésirable ou du spam.

2. Choisissez Renvoyer le code, actualisez votre boîte de réception et vérifiez à nouveau vos dossiers de spam, de courrier indésirable et d'éléments supprimés.
3. Si vous ne voyez toujours pas votre e-mail de vérification, vérifiez que votre adresse e-mail AWS Builder ID ne contient pas de fautes de frappe. Si vous avez saisi la mauvaise adresse e-mail, réinscrivez-vous avec une adresse e-mail que vous possédez.

Je n'arrive pas à me connecter avec Google

Si vous possédez déjà un ID de constructeur AWS profil avec la même adresse e-mail que votre compte Google, utilisez votre ID de constructeur AWS mot de passe pour vous connecter à votre

compte. Si vous ne vous souvenez pas de votre mot de passe, consultezJ'ai oublié mon mot de passe.

Pour obtenir de l'aide pour vous connecter à l'aide de votre mot de passe Google, consultez Impossible de vous connecter à votre compte Google.

Je n'arrive pas à me connecter avec Apple

Si vous possédez déjà un ID de constructeur AWS profil avec la même adresse e-mail que votre compte Apple, utilisez votre ID de constructeur AWS mot de passe pour vous connecter à votre compte. Si vous ne vous souvenez pas de votre mot de passe, consultezJ'ai oublié mon mot de passe.

Pour obtenir de l'aide pour vous connecter à l'aide de votre mot de passe Apple, consultez Si vous ne parvenez pas à vous connecter à votre compte Apple.

Je n'arrive pas à me connecter avec GitHub

Si vous avez déjà un ID de constructeur AWS profil avec la même adresse e-mail que votre GitHub compte, utilisez votre ID de constructeur AWS mot de passe pour vous connecter à votre compte. Si vous ne vous souvenez pas de votre mot de passe, consultezJ'ai oublié mon mot de passe.

Pour obtenir de l'aide pour vous connecter avec votre GitHub mot de passe, voir Impossible de se connecter - GitHub Support.

Je n'arrive pas à me connecter avec Amazon

Si vous possédez déjà un ID de constructeur AWS profil avec la même adresse e-mail que votre compte Amazon, utilisez votre ID de constructeur AWS mot de passe pour vous connecter à votre compte. Si vous ne vous souvenez pas de votre mot de passe, consultezJ'ai oublié mon mot de passe.

Pour obtenir de l'aide pour vous connecter avec votre mot de passe Amazon, consultez la section Aide à la connexion.

J'ai reçu un message d'erreur de connexion lorsque j'ai essayé de m'inscrire ID de constructeur AWS pour continuer avec Google

Cela signifie soit que vous possédez déjà une adresse e-mail ID de constructeur AWS utilisant la même adresse e-mail que votre compte Google, soit que l'adresse e-mail associée à votre compte Google n'est pas vérifiée. Dans les deux cas, essayez de vous réinscrire en saisissant votre adresse e-mail et en fournissant un mot de passe.

J'ai reçu un message d'erreur de connexion lorsque j'ai essayé de m'inscrire pour continuer à ID de constructeur AWS utiliser Apple

Cela signifie soit que vous possédez déjà ID de constructeur AWS une adresse e-mail identique à celle de votre compte Apple, soit que l'adresse e-mail associée à votre compte Apple n'est pas vérifiée ou gérée par votre entreprise avec Apple Business Manager ou par votre établissement avec Apple School Manager. Dans les deux cas, essayez de vous réinscrire en saisissant votre adresse e-mail et en fournissant un mot de passe.

J'ai reçu une erreur de connexion lorsque j'ai essayé de m'inscrire pour ID de constructeur AWS utiliser Continue with GitHub

Cela signifie soit que vous possédez déjà une adresse e-mail ID de constructeur AWS utilisant la même adresse e-mail que votre GitHub compte, soit que l'adresse e-mail associée à votre GitHub compte n'est pas vérifiée. Dans les deux cas, essayez de vous réinscrire en saisissant votre adresse e-mail et en fournissant un mot de passe.

J'ai reçu un message d'erreur de connexion lorsque j'ai essayé de m'inscrire pour continuer à ID de constructeur AWS utiliser Amazon

Cela signifie soit que vous possédez déjà une adresse e-mail ID de constructeur AWS utilisant la même adresse e-mail que votre compte Amazon, soit que l'adresse e-mail associée à votre compte Amazon n'est pas vérifiée. Dans les deux cas, essayez de vous réinscrire en saisissant votre adresse e-mail et en fournissant un mot de passe.

Je reçois un message d'erreur indiquant « Ce n'est pas toi, c'est nous » lorsque j'essaie de me connecter avec mon ID de constructeur AWS

Si vous recevez ce message d'erreur lorsque vous essayez de vous connecter, il se peut qu'il y ait un problème avec vos paramètres locaux ou votre adresse e-mail.

- Vérifiez les paramètres de date et d'heure sur l'appareil que vous utilisez pour vous connecter. Nous vous recommandons d'autoriser le réglage automatique de la date et de l'heure. Si ce n'est pas le cas, nous vous recommandons de synchroniser la date et l'heure avec un serveur NTP (Network Time Protocol) connu.
- Vérifiez votre adresse e-mail pour détecter les erreurs de formatage. Les problèmes suivants renverront un message d'erreur lorsque vous tenterez de vous connecter avec votre ID de constructeur AWS.
  - Espace dans une adresse e-mail
  - Barre oblique (/) dans une adresse e-mail
  - Deux points (.) dans une adresse e-mail
  - Deux esperluettes (@) dans une adresse e-mail
  - Virgule (,) à la fin d'une adresse e-mail
  - Crochet (]) à la fin d'une adresse e-mail

J'ai oublié mon mot de passe

Pour réinitialiser votre mot de passe oublié

1. Sur la page Se connecter avec AWS Builder ID, entrez l'e-mail que vous avez utilisé pour créer votre AWS Builder ID dans Adresse e-mail. Choisissez Suivant.
2. Choisissez Mot de passe oublié ? . Nous envoyons un lien à l'adresse e-mail associée à votre identifiant AWS Builder où vous pouvez réinitialiser votre mot de passe.
3. Suivez les instructions de l'e-mail.

Je n'arrive pas à définir un nouveau mot de passe

Pour votre sécurité, vous devez respecter les exigences suivantes chaque fois que vous définissez ou modifiez votre mot de passe :

- Les mots de passe distinguent majuscules et minuscules.
- Les mots de passe doivent comporter entre 8 et 64 caractères.
- Les mots de passe doivent contenir au moins un caractère appartenant à chacune des quatre catégories suivantes :
  - Lettres minuscules (a-z)
  - Lettres majuscules (A-Z)
  - Chiffres (0-9)
  - Caractères non alphanumériques (~ ! @#$%^portail de gestion*_-+=`| \ () {} [] : ; "'<>,. ? /)
- Les trois derniers mots de passe ne peuvent pas être réutilisés.
- Les mots de passe connus du public grâce à un ensemble de données divulgué par un tiers ne peuvent pas être utilisés.

Mon mot de passe ne fonctionne pas

Si vous vous souvenez de votre mot de passe, mais qu'il ne fonctionne pas lorsque vous vous connectez avec AWS Builder ID, assurez-vous que :

- Le verrouillage des majuscules est désactivé.
- Vous n'utilisez pas un ancien mot de passe.
- Vous utilisez votre mot de passe AWS Builder ID et non un mot de passe pour un Compte AWS.

Si vous vérifiez que votre mot de passe est up-to-date bien entré, mais qu'il ne fonctionne toujours pas, suivez les instructions J'ai oublié mon mot de passe pour réinitialiser votre mot de passe.

Mon mot de passe ne fonctionne pas et je ne peux plus accéder aux e-mails envoyés à mon adresse e-mail AWS Builder ID

Si vous pouvez toujours vous connecter à votre identifiant AWS Builder, utilisez la page de profil pour mettre à jour votre adresse e-mail AWS Builder ID vers votre nouvelle adresse e-mail. Une fois la

vérification des e-mails terminée, vous pouvez vous connecter à votre nouvelle adresse e-mail AWS et recevoir des communications à cette adresse.

Si vous avez utilisé une adresse e-mail professionnelle ou universitaire, que vous avez quitté l'entreprise ou l'école et que vous ne pouvez recevoir aucun e-mail envoyé à cette adresse, contactez l'administrateur de ce système de messagerie. Ils peuvent être en mesure de transférer votre e-mail vers une nouvelle adresse, de vous accorder un accès temporaire ou de partager le contenu de votre boîte aux lettres.

Je ne parviens pas à activer le MFA

Pour activer le MFA, ajoutez un ou plusieurs appareils MFA à votre profil en suivant les étapes décrites dans. Gérer l'authentification ID de constructeur AWS multifactorielle (MFA)

Je ne parviens pas à ajouter une application d'authentification en tant qu'appareil MFA

Si vous ne pouvez pas ajouter un autre appareil MFA, vous avez peut-être atteint le nombre maximal d'appareils MFA que vous pouvez enregistrer dans cette application. Essayez de supprimer un appareil MFA non utilisé ou d'utiliser une autre application d'authentification.

Je ne parviens pas à supprimer un appareil MFA

Si vous avez l'intention de désactiver le MFA, procédez au retrait de votre appareil MFA en suivant les étapes décrites dans. Supprimer votre appareil MFA Toutefois, si vous souhaitez que l'authentification MFA reste activée, vous devez ajouter un autre périphérique MFA avant de tenter de supprimer un périphérique MFA existant. Pour plus d'informations sur l'ajout d'un autre périphérique MFA, consultez. Gérer l'authentification ID de constructeur AWS multifactorielle (MFA)

Je reçois le message « Une erreur inattendue s'est produite » lorsque j'essaie de m'inscrire ou de me connecter avec une application d'authentification

Un système de mot de passe à usage unique basé sur le temps (TOTP), tel que celui utilisé par AWS Builder ID en combinaison avec une application d'authentification basée sur le code, repose sur la

synchronisation de l'heure entre le client et le serveur. Assurez-vous que l'appareil sur lequel votre application d'authentification est installée est correctement synchronisé avec une source de temps fiable, ou réglez manuellement l'heure sur votre appareil pour qu'elle corresponde à une source fiable, telle que le NIST ou d'autres équivalents. local/regional

Je reçois le message « Ce n'est pas toi, c'est nous » lorsque j'essaie de me connecter à AWS Builder ID

Vérifiez les paramètres de date et d'heure sur l'appareil que vous utilisez pour vous connecter. Nous vous recommandons de définir la date et l'heure à régler automatiquement. Si ce n'est pas le cas, nous vous recommandons de synchroniser la date et l'heure avec un serveur NTP (Network Time Protocol) connu.

Me déconnecter ne me déconnecte pas complètement

Le système est conçu pour vous déconnecter immédiatement, mais la déconnexion complète peut prendre jusqu'à une heure.

> **Note**
>
> Lorsque vous utilisez un compte de connexion sociale tel que Google ou Apple, la suppression de ID de constructeur AWS sessions actives ne vous déconnecte pas de votre compte de connexion sociale.

Je cherche toujours à résoudre mon problème

Vous pouvez remplir le formulaire de commentaires relatifs au Support. Dans la section Demande d'informations, sous Comment pouvons-nous vous aider, indiquez que vous utilisez AWS Builder ID. Fournissez le plus de détails possible afin que nous puissions résoudre votre problème le plus efficacement possible.

AWS politiques gérées pour Connexion à AWS

Une politique AWS gérée est une politique autonome créée et administrée par AWS. AWS les politiques gérées sont conçues pour fournir des autorisations pour de nombreux cas d'utilisation courants afin que vous puissiez commencer à attribuer des autorisations aux utilisateurs, aux groupes et aux rôles.

N'oubliez pas que les politiques AWS gérées peuvent ne pas accorder d'autorisations de moindre privilège pour vos cas d'utilisation spécifiques, car elles sont accessibles à tous les AWS clients. Nous vous recommandons de réduire encore les autorisations en définissant des politiques gérées par le client qui sont propres à vos cas d'utilisation.

Vous ne pouvez pas modifier les autorisations définies dans les politiques AWS gérées. Si les autorisations définies dans une politique AWS gérée sont AWS mises à jour, la mise à jour affecte toutes les identités principales (utilisateurs, groupes et rôles) auxquelles la politique est attachée. AWS est le plus susceptible de mettre à jour une politique AWS gérée lorsqu'une nouvelle Service AWS est lancée ou lorsque de nouvelles opérations d'API sont disponibles pour les services existants.

Pour plus d'informations, consultez Politiques gérées par AWS dans le Guide de l'utilisateur IAM.

AWS politique gérée : AmazonManagedSignUpServicePolicy

La `AmazonManagedSignUpServicePolicy` politique accorde les autorisations nécessaires pour terminer les processus d'inscription au AWS compte.

Vous pouvez associer `AmazonManagedSignUpServicePolicy` à vos utilisateurs, groupes et rôles.

Détails de l'autorisation

Cette politique inclut les autorisations suivantes :

- Vérification du client : permet de créer, de récupérer et de mettre à jour les informations de vérification et le statut d'éligibilité du client, notamment en créant des URL de téléchargement pour les documents de vérification.

Pour plus de détails sur cette politique, y compris la dernière version du document sur la politique JSON, consultez AmazonManagedSignUpServicePolicy dans le Guide de référence de la politique gérée par AWS .

AWS politique gérée : ApplicationProvisioningPolicy

La ApplicationProvisioningPolicy politique accorde des autorisations complètes pour le provisionnement des applications et les opérations de gestion des identités, y compris la gestion des rôles et des politiques IAM, la configuration SSO et les opérations du magasin d'identités.

Vous pouvez associer `ApplicationProvisioningPolicy` à vos utilisateurs, groupes et rôles.

Détails de l'autorisation

Cette politique inclut les autorisations suivantes :

- Gestion IAM : permet des opérations IAM complètes, notamment la création, la mise à jour et la suppression de rôles et de politiques, la gestion des pièces jointes aux rôles et la création de rôles liés à un service.
- Studio de recherche et d'ingénierie sur AWS- Autorise toutes les opérations sur les Studio de recherche et d'ingénierie sur AWS ressources.
- Transfert de rôles : permet de transmettre des rôles IAM à d'autres services.
- IAM Identity Center : permet de gérer les instances, les applications, les attributions, les autorisations et les méthodes d'authentification IAM Identity Center.
- Identity Store : permet de lire les informations relatives aux utilisateurs et aux groupes depuis l'Identity Store.
- IAM Identity Center OAuth - Permet d'authentifier les sessions IAM via IAM Identity Center OAuth.
- Profil utilisateur et répertoire - Permet de gérer les connecteurs IAM Identity Center, les profils utilisateur et les configurations d'annuaire, y compris la configuration du fournisseur d'identité externe.
- Abonnements utilisateurs - Permet de répertorier les abonnements des utilisateurs.

Pour plus de détails sur cette politique, y compris la dernière version du document sur la politique JSON, consultez ApplicationProvisioningPolicy dans le Guide de référence de la politique gérée par AWS .

AWS politique gérée : SignInLocalDevelopmentAccess

La `SignInLocalDevelopmentAccess` politique accorde des autorisations d'accès programmatique à l' AWS aide des informations d'identification de votre console.

Vous pouvez associer `SignInLocalDevelopmentAccess` à vos utilisateurs, groupes et rôles.

Détails de l'autorisation

Cette politique inclut les autorisations suivantes :

- Autorisation de l'accès à OAuth2 : autorise l'authentification via un navigateur et l'obtention d'un code d'autorisation OAuth 2.0 pour l'échange d'informations d'identification
- Création d'un jeton OAuth2 : autorise l'échange d'un code d'autorisation contre un jeton d'accès OAuth 2.0 et un jeton d'actualisation qui peuvent être utilisés pour accéder aux AWS services à partir d'outils et d'applications de développement

> **Note**
>
> L'ajout de cette politique AWS gérée vous donne l'autorisation d'effectuer une authentification à la fois sur le même appareil et sur plusieurs appareils. Cette politique autorise les actions sur les ressources suivantes :
>
> - `arn:aws:signin:`*`region`*`:`*`account-id`*`:oauth2/public-client/localhost`— Utilisé pour l'authentification sur le même appareil avec. `aws login`
> - `arn:aws:signin:`*`region`*`:`*`account-id`*`:oauth2/public-client/remote`— Utilisé pour l'authentification multi-appareils avec`aws login --remote`.
>
> Pour contrôler l'accès à l'une ou l'autre méthode d'authentification, vous pouvez créer votre propre politique gérée ou votre propre politique de contrôle des services (SCP). Utilisez ces ARN de ressources pour autoriser ou refuser l'accès programmatique à AWS à l'aide des informations d'identification de votre console.

Pour de plus amples informations, veuillez consulter Connectez-vous avec les informations d'identification de la console (recommandé). Pour plus de détails sur cette politique, y compris la dernière version du document sur la politique JSON, consultez SignInLocalDevelopmentAccess dans le Guide de référence de la politique gérée par AWS .

AWS politique gérée : AWSSignInResourcePolicyManagement

La `AWSSignInResourcePolicyManagement` politique accorde des autorisations pour gérer la configuration des autorisations de console et les déclarations d'autorisation des ressources pour AWS Sign-In.

Vous pouvez associer `AWSSignInResourcePolicyManagement` à vos utilisateurs, groupes et rôles.

Détails de l’autorisation

Cette politique inclut les autorisations suivantes :

- `signin:PutConsoleAuthorizationConfiguration`— Créez ou mettez à jour les paramètres d'autorisation de la console.
- `signin:GetConsoleAuthorizationConfiguration`— Récupère la configuration d'autorisation actuelle de la console.
- `signin:DeleteConsoleAuthorizationConfiguration`— Supprimez la configuration d'autorisation de la console.
- `signin:PutResourcePermissionStatement`— Créez ou mettez à jour des déclarations d'autorisation relatives aux ressources.
- `signin:DeleteResourcePermissionStatement`— Supprime les déclarations d'autorisation relatives aux ressources.
- `signin:ListResourcePermissionStatements`— Répertorie les déclarations d'autorisation relatives aux ressources pour le compte.
- `signin:GetResourcePolicy`— Récupérez la politique consolidée basée sur les ressources.

Voici la politique JSON :

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "signin:PutConsoleAuthorizationConfiguration",
                "signin:GetConsoleAuthorizationConfiguration",
                "signin:DeleteConsoleAuthorizationConfiguration",
```

```
                "signin:PutResourcePermissionStatement",
                "signin:DeleteResourcePermissionStatement",
                "signin:ListResourcePermissionStatements",
                "signin:GetResourcePolicy"
            ],
            "Resource": "*"
        }
    ]
}
```

Associez cette politique aux principaux IAM (utilisateurs ou rôles) qui gèrent les politiques basées sur les ressources pour. AWS Sign-In Cela inclut les administrateurs de sécurité chargés de configurer les contrôles d'accès basés sur le réseau, les responsables de la conformité qui doivent auditer les politiques d'accès à la console et les équipes opérationnelles qui gèrent les configurations d'accès pour la restauration d'urgence.

> **Important**
>
> Cette politique accorde un accès administratif aux contrôles d'autorisation de la console. Appliquez le principe du moindre privilège lors de l'attribution de cette politique. Envisagez d'utiliser des conditions IAM pour restreindre davantage le moment et la manière dont ces autorisations peuvent être utilisées.

Pour plus de détails sur cette politique, y compris la dernière version du document sur la politique JSON, consultez AWSSignInResourcePolicyManagement dans le Guide de référence de la politique gérée par AWS .

Connexion à AWS mises à jour de AWS stratégies gérées

Consultez les détails des mises à jour des politiques AWS gérées Connexion à AWS 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 Historique du Connexion à AWS document.

Modifier	Description	Date
AWSSignInResourceP olicyManagement : nouvelle politique	Ajout d'une nouvelle politique AWS gérée qui accorde des autorisations pour gérer la configuration des autorisations de console et les déclarations d'autorisation des ressources pour AWS Sign-In.	10 juin 2026
SignInLocalDevelop mentAccess : nouvelle politique	Ajout d'une nouvelle politique AWS gérée qui accorde des autorisations d'accès programmatique à AWS l'aide de vos informations d'identif ication de console existantes.	19 novembre 2025
ApplicationProvisioningPolicy : nouvelle politique	Ajout d'une nouvelle politique AWS gérée qui accorde des autorisations complètes pour le provisionnement des applications et les opération s de gestion des identités , y compris la gestion des rôles et des politiques IAM, la configuration du centre d'identité IAM et les opérations du magasin d'identités.	30 septembre 2025
AmazonManagedSignU pServicePolicy : nouvelle politique	Ajout d'une nouvelle politique AWS gérée qui accorde les autorisations requises pour les processus d'ouverture de AWS compte, y compris les opérations de vérification client et de configuration des paiements.	30 septembre 2025

Modifier	Description	Date
Connexion à AWS a commencé à suivre les modifications	Connexion à AWS a commencé à suivre les modifications apportées AWS à ses politiques gérées.	30 septembre 2025

Historique du document

Le tableau suivant décrit les ajouts importants à la AWS Sign-In documentation. Nous mettons aussi la documentation à jour régulièrement pour prendre en compte les commentaires qui nous sont envoyés.

- Dernière mise à jour majeure de la documentation : 10 juin 2026

Modification	Description	Date
Support pour les politiques Sign-in basées sur les ressources et les politiques de contrôle des ressources	Ajout d'une documentation pour contrôler l' AWS Management Console accès à l'aide de politiques Sign-in basées sur les ressources et de politiques de contrôle des ressources (RCP), d'une nouvelle référence aux clés de condition, de la politique `AWSSignInResourcePolicyManagement` gérée et de résolution des problèmes associés.	10 juin 2026
Support pour Sign in with GitHub et Amazon	Connexion à AWS prend désormais en charge la connexion avec Amazon GitHub et la connexion avec Amazon afin que vous puissiez créer un compte ID de constructeur AWS en utilisant votre compte GitHub ou Amazon.	10 mars 2026
Support pour la connexion avec Apple	Connexion à AWS prend désormais en charge la	5 février 2026

	connexion avec Apple afin que vous puissiez en créer un ID de constructeur AWS à l'aide de votre compte Apple. ID de constructeur AWS rubriques mises à jour et nouvelles rubriques de résolution des problèmes ajoutées à la section Résolution ID de constructeur AWS des problèmes.	
Nouvelle politique gérée	Connexion à AWS a publié une nouvelle politique gérée. `SignInLocalDevelopmentAccess` accorde des autorisations d'accès programmatique pour un accès programmatique à l' AWS aide de vos informations d'identification de console existantes. Pour plus d'informations, voir les Connexion à AWS mises à jour des politiques AWS gérées.	19 novembre 2025

Support pour la connexion avec Google	Connexion à AWS prend désormais en charge la connexion avec Google afin que vous puissiez en créer un ID de constructeur AWS à l'aide de votre compte Google. ID de constructeur AWS rubriques mises à jour et nouvelles rubriques de résolution des problèmes ajoutées à la section Résolution ID de constructeur AWS des problèmes.	30 septembre 2025
Nouvelles politiques gérées	Connexion à AWS a publié deux nouvelles politiques gérées. `AmazonManagedSignUpServicePolicy` accorde les autorisations nécessaires pour terminer les processus d'inscription au AWS compte. `ApplicationProvisioningPolicy` accorde des autorisations complètes pour le provisionnement des applications et les opérations de gestion des identités. Pour plus d'informations, voir les Connexion à AWS mises à jour des politiques AWS gérées.	30 septembre 2025

Rubriques de dépannage mises à jour	Ajout de nouvelles rubriques de résolution des problèmes pour la connexion ID de constructeur AWS et le AWS Management Console.	27 février 2024
Plusieurs rubriques d'organisation ont été mises à jour	Types d'utilisateurs mis à jour, supprimés Déterminer le type d'utilisateur et incorporation de son contenu dans les types d'utilisateurs, comment se connecter à AWS	15 mai 2023
Mise à jour de plusieurs sujets et de la bannière supérieure	Types d'utilisateurs mis à jour, détermination du type d'utilisateur, comment se connecter AWS, qu'est-ce que c'est AWS Sign-in ? . Les procédures de connexion des utilisateurs root et IAM ont également été mises à jour.	3 mars 2023
Paragraphe d'introduction mis à jour pour la AWS Management Console connexion	Déplacé Determine le type d'utilisateur en haut de la page et suppression de la note qui existe dans Account root user.	27 février 2023
Ajouté ID de constructeur AWS	Des ID de constructeur AWS rubriques ont été ajoutées au guide de AWS Sign-In l'utilisateur et du contenu a été intégré aux rubriques existantes.	31 janvier 2023

Mise à jour organisationnelle	Sur la base des commentaires des clients, la table des matières a été mise à jour pour clarifier les méthodes de connexion. Mise à jour des didacticiels de connexion. Terminologie mise à jour et détermination du type d'utilisateur. Liaison croisée améliorée pour définir des termes tels que utilisateur IAM et utilisateur root.	22 décembre 2022
Nouveau guide	Il s'agit de la première version du guide de AWS Sign-In l'utilisateur.	31 août 2022

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.