aws

Guide de l’utilisateur

Console Outils pour développeur

Console Outils pour développeur: Guide de l’utilisateur

Table of Contents

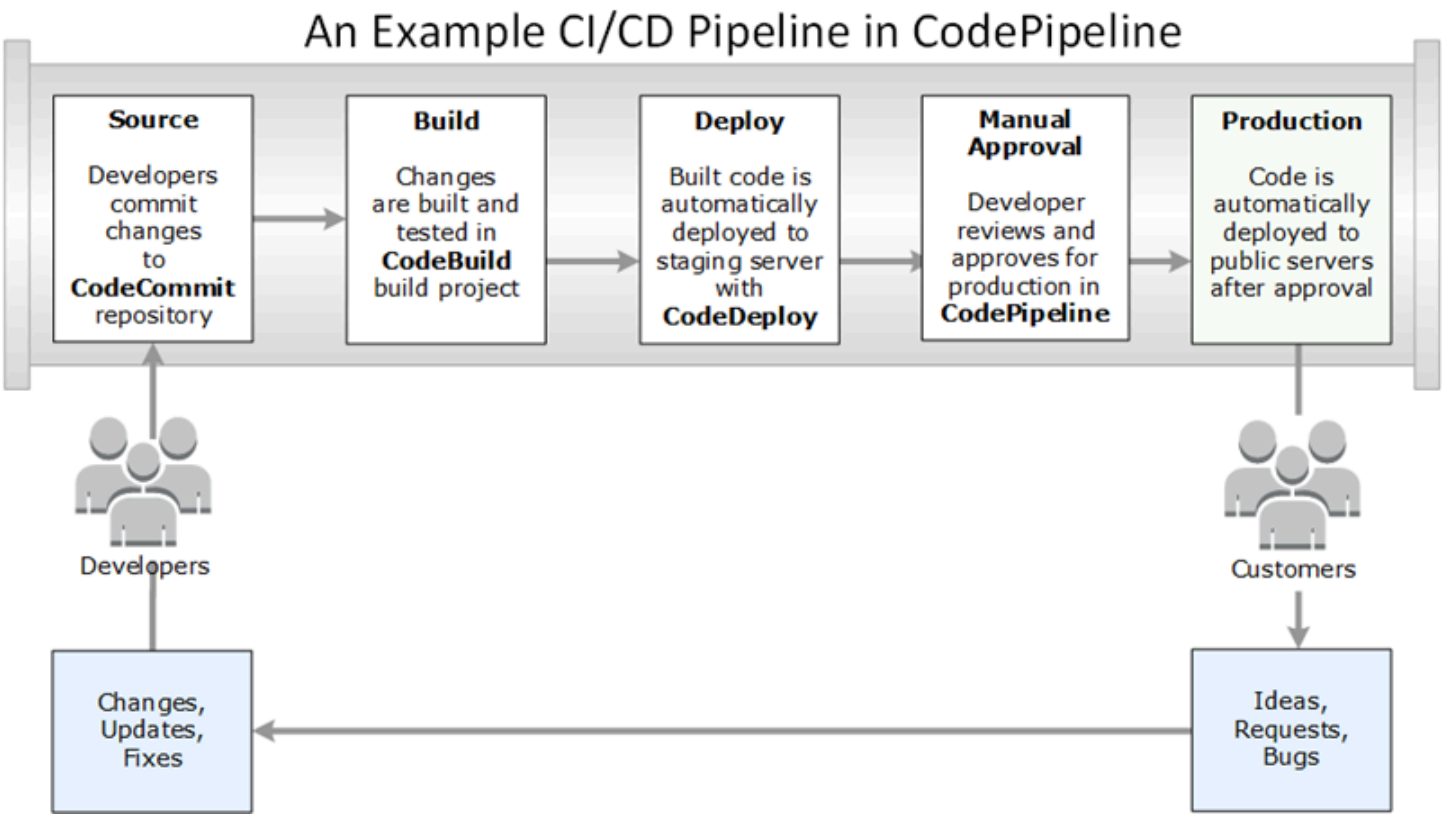
Présentation de la console Outils pour développeurs

La console Outils pour développeurs héberge un ensemble de services et de fonctions que vous pouvez utiliser individuellement ou collectivement pour vous aider à développer des logiciels, individuellement ou en équipe. Les outils pour développeurs peuvent vous aider à stocker, créer, tester et déployer votre logiciel en toute sécurité. Utilisés individuellement ou collectivement, ces outils prennent en charge DevOps, l'intégration continue et la livraison continue (CI/CD).

La console Outils pour développeurs comprend les services suivants :

- AWS CodeCommit est un service de contrôle de code source entièrement géré qui héberge des référentiels Git privés. Vous pouvez créer un référentiel pour stocker et gérer de manière privée les ressources (telles que des documents, du code source et des fichiers binaires) dans le AWS Cloud. Vos référentiels stockent l'historique de votre projet, à partir de la première validation jusqu'aux dernières modifications. Vous pouvez travailler en collaboration sur le code dans les référentiels en commentant le code et en créant des requêtes d'extraction pour garantir la qualité du code.
- AWS CodeBuild est un service de génération entièrement géré qui compile votre code source, exécute des tests unitaires et produit des artefacts prêts à déployer. Ce service fournit des environnements de génération prépackagés pour les langages de programmation et outils de génération couramment utilisés, comme Apache Maven, Gradle, etc. Vous pouvez également personnaliser des environnements de génération dans CodeBuild pour utiliser vos propres outils de génération.
- AWS CodeDeploy est un service de déploiement entièrement géré qui automatise les déploiements de logiciels vers des services de calcul tels qu'Amazon EC2, AWS Lambda et vos serveurs sur site. Il peut vous aider à publier rapidement de nouvelles fonctionnalités, à éviter les temps d'arrêt pendant le déploiement des applications et à gérer la complexité de la mise à jour de vos applications.
- AWS CodePipeline est un service de diffusion en continu qui permet de modéliser, visualiser et automatiser les étapes nécessaires à la publication de vos logiciels. Vous pouvez rapidement modéliser et configurer différentes étapes d'un processus de publication logiciel. Vous pouvez créer, tester et déployer votre code dès que ce dernier est modifié, selon les modèles de traitement des versions que vous définissez.

Voici un exemple de la façon dont vous pouvez utiliser les services dans la console Outils pour développeurs et vous aider à développer des logiciels.



Dans cet exemple, les développeurs créent un référentiel dans CodeCommit et l'utilisent pour développer et collaborer sur leur code. Ils créent un projet de génération dans CodeBuild pour générer et tester leur code, et utilisent CodeDeploy pour déployer leur code sur les environnements de test et de production. Ils veulent itérer rapidement, de sorte qu'ils créent un pipeline dans CodePipeline pour détecter les modifications dans le référentiel CodeCommit. Ces modifications sont générées, les tests sont exécutés et le code développé et testé avec succès est déployé sur le serveur de test. L'équipe ajoute des étapes de test au pipeline pour exécuter d'autres tests sur le serveur intermédiaire, tels que des tests d'intégration ou de chargement. Une fois ces tests terminés avec succès, un membre de l'équipe examine les résultats et, s'il est satisfait, approuve manuellement les modifications pour la production. CodePipeline déploie le code testé et approuvé sur les instances de production.

Ce n'est qu'un exemple simple de la façon dont vous pouvez utiliser un ou plusieurs des services disponibles dans la console Outils pour développeurs pour vous aider à développer des logiciels. Chacun des services peut être personnalisé pour répondre à vos besoins. Ils offrent de nombreuses intégrations à d'autres produits et services, à la fois dans AWS et dans d'autres outils tiers. Pour plus d'informations, consultez les rubriques suivantes :

- CodeCommit : intégrations de produits et services

- CodeBuild :utilisation de CodeBuild avec Jenkins
- CodeDeploy : intégrations de produits et services
- CodePipeline :intégrations de produits et services

Est-ce votre première utilisation ?

Si vous utilisez pour la première fois un ou plusieurs des services disponibles dans la console Outils pour développeurs, nous vous recommandons de commencer par lire les rubriques suivantes :

- Premiers pas avec CodeCommit
- Premiers pas avec CodeBuild, Concepts
- Premiers pas avec CodeDeploy, Composants principaux
- Premiers pas avec CodePipeline, Concepts

Caractéristiques de la console Outils pour développeurs

La console Outils pour développeurs comprend les fonctions suivantes :

- La console Outils pour développeurs inclut une fonction de gestionnaire de notifications que vous pouvez utiliser pour vous abonner aux événements dans AWS CodeBuild, AWS CodeCommit, AWS CodeDeploy et AWS CodePipeline. Cette fonction a sa propre API, AWS CodeStar Notifications. Vous pouvez utiliser la fonctionnalité de notifications pour informer rapidement les utilisateurs des événements dans les référentiels, les projets de construction, les applications de déploiement et les pipelines les plus importants pour leur travail. Un gestionnaire de notifications aide les utilisateurs à prendre conscience des événements qui se produisent sur les référentiels, les builds, les déploiements ou les pipelines afin qu'ils puissent rapidement prendre des mesures, telles que l'approbation de modifications ou la correction d'erreurs. Pour plus d'informations, consultez Que sont les notifications ?.
- La console Outils pour développeurs inclut une fonction de connexion que vous pouvez utiliser pour associer vos ressources AWS à des fournisseurs de code source tiers. Cette fonction a sa propre API, AWS CodeStar Connections. Vous pouvez utiliser la fonction de connexion pour configurer une connexion autorisée avec un fournisseur tiers et utiliser la ressource de connexion avec d'autres services AWS. Pour plus d'informations, consultez Qu'est-ce que les connexions ?.

Que sont les notifications ?

La fonction de notifications dans dans la console Outils pour développeurs est un gestionnaire de notifications permettant de s'abonner aux événements dans AWS CodeBuild, AWS CodeCommit, AWS CodeDeploy et AWS CodePipeline. Cette fonction a sa propre API, AWS CodeStar Notifications. Vous pouvez utiliser la fonctionnalité de notifications pour informer rapidement les utilisateurs des événements dans les référentiels, les projets de construction, les applications de déploiement et les pipelines les plus importants pour leur travail. Un gestionnaire de notifications aide les utilisateurs à prendre conscience des événements qui se produisent sur les référentiels, les builds, les déploiements ou les pipelines afin qu'ils puissent rapidement prendre des mesures, telles que l'approbation de modifications ou la correction d'erreurs.

Que puis-je faire avec les notifications ?

Vous pouvez utiliser les notifications pour créer et gérer des règles de notification afin d'avertir automatiquement les utilisateurs des modifications importantes apportées à leurs ressources, notamment :

- Réussites et échecs de génération dans les projets de génération CodeBuild.
- Réussites et échecs du déploiement dans les applications CodeDeploy.
- Création et mises à jour des demandes d'extraction, y compris des commentaires sur le code, dans les référentiels CodeCommit.
- Statuts d'approbation manuelle et exécutions de pipeline dans CodePipeline.

Vous pouvez configurer les notifications de sorte qu'elles soient envoyées aux adresses e-mail des utilisateurs abonnés à une rubrique Amazon SNS. Vous pouvez également configurer l'intégration à AWS Chatbot et faire en sorte que les notifications soient envoyées aux canaux Slack, au canal Microsoft Teams ou aux salles de conversation Amazon Chime.

Comment fonctionnent les notifications ?

Lorsque vous configurez une règle de notification pour une ressource prise en charge, telle qu'un référentiel, un projet de génération, une appli ou un pipeline, la fonctionnalité de notification crée une règle Amazon EventBridge qui surveille les événements que vous spécifiez. Lorsqu'un événement de ce type se produit, la règle de notification envoie des notifications aux rubriques Amazon SNS spécifiées comme cibles de cette règle. Les abonnés à ces cibles reçoivent des notifications à propos de ces événements.

Comment commencer avec les notifications ?

Pour commencer, voici quelques rubriques utiles à consulter :

- Découvrez les concepts pour les notifications.
- Configurez les ressources dont vous avez besoin pour commencer à utiliser les notifications.
- Démarrez avec vos premières règles de notification et recevez vos premières notifications.

Concepts de notification

Vous trouverez la configuration et l'utilisation des notifications plus simples si vous comprenez les concepts et les termes. Voici quelques concepts à connaître lorsque vous utilisez les notifications.

Rubriques

- Notifications
- Règles de notification
- Événements
- Types de détails
- Cibles
- Notifications et AWS CodeStar Notifications
- Événements pour les règles de notification sur les référentiels
- Événements pour les règles de notification sur les projets de génération
- Événements pour les règles de notification sur les applications de déploiement
- Événements pour les règles de notification sur les pipelines

Notifications

Une notification est un message qui contient des informations sur les événements qui se produisent dans les ressources que vous et vos développeurs utilisez. Vous pouvez configurer des notifications afin que les utilisateurs d'une ressource, comme un projet de génération, un référentiel, une application de déploiement ou un pipeline, reçoivent des e-mails sur les types d'événements que vous spécifiez en fonction de la règle de notification que vous créez.

Les notifications pour AWS CodeCommit peuvent contenir des informations sur l'identité de l'utilisateur, telles qu'un nom complet ou une adresse e-mail, grâce à l'utilisation de balises de

session. CodeCommit prend en charge l'utilisation de balises de session, qui sont des attributs de paire clé-valeur que vous transmettez lorsque vous assumez un rôle IAM, utilisez les informations d'identification temporaires ou fédérez un utilisateur dans AWS Security Token Service (AWS STS). Vous pouvez également associer des balises à un utilisateur IAM. CodeCommit inclut les valeurs pour `displayName` et `emailAddress` dans le contenu de notification si ces balises sont présentes. Pour plus d'informations, consultez Utilisation de balises pour fournir des informations d'identité supplémentaires dans CodeCommit.

> **Important**
>
> Les notifications incluent des informations spécifiques au projet, telles que les statuts de génération et de déploiement, les lignes de code contenant des commentaires et les approbations de pipeline. Le contenu des notifications peut changer à mesure que de nouvelles fonctionnalités sont ajoutées. En tant que bonne pratique en matière de sécurité, vous devriez examiner régulièrement les cibles des règles de notification et les abonnés de la rubrique Amazon SNS. Pour de plus amples informations, veuillez consulter Présentation du contenu des notifications et de la sécurité.

Règles de notification

Une règle de notification est une ressource AWS que vous créez pour spécifier quand et où les notifications sont envoyées. Elle définit :

- Les conditions dans lesquelles une notification est créée. Ces conditions sont basées sur les événements que vous choisissez, qui sont spécifiques au type de ressource. Les types de ressources pris en charge incluent les projets de génération dans AWS CodeBuild, les applications de déploiement dans AWS CodeDeploy, les pipelines dans AWS CodePipeline et les référentiels dans AWS CodeCommit.
- Les cibles auxquelles la notification est envoyée. Vous pouvez spécifier jusqu'à 10 cibles pour une règle de notification.

Les règles de notification sont étendues aux projets de construction individuels, aux applications de déploiement, aux pipelines et aux référentiels. Les règles de notification ont des noms conviviaux définis par l'utilisateur et des noms ARN (Amazon Resource Name). Les règles de notification ne peuvent être créées que dans la même région AWS que celle où la ressource existe. Par exemple,

si votre projet de génération se trouve dans la région USA Est (Ohio), votre règle de notification doit également être créée dans la région USA Est (Ohio).

Vous pouvez définir jusqu'à 10 règles de notification pour une ressource.

Événements

Un événement est un changement d'état sur une ressource que vous souhaitez surveiller. Chaque ressource possède une liste de types d'événements que vous pouvez choisir. Lorsque vous configurez une règle de notification sur une ressource, vous spécifiez les événements qui entraîneront l'envoi de notifications lorsqu'ils se produiront. Par exemple, si vous configurez des notifications pour un référentiel dans CodeCommit et que vous sélectionnez Created (Créé) pour Pull request (Demande d'extraction) et Branches and tags (Branches et balises), une notification est envoyée chaque fois qu'un utilisateur de ce référentiel crée une demande d'extraction, une branche ou une balise Git.

Types de détails

Lorsque vous créez une règle de notification, vous pouvez choisir le niveau de détail ou le type de détail inclus dans les notifications (Total ou Basique). Le paramètre Total (valeur par défaut) inclut toutes les informations disponibles pour l'événement dans la notification, y compris toute information améliorée fournie par les services pour des événements spécifiques. Le paramètre Basique inclut uniquement un sous-ensemble des informations disponibles.

Le tableau suivant répertorie les informations améliorées disponibles pour des types d'événements spécifiques et décrit les différences entre les types de détails.

Service	Événement	L'option Total inclut	L'option Basique n'inclut pas
CodeCommit	Commentaires sur les validations Commentaires sur les demandes d'extraction	Tous les détails de l'événement et le contenu du commentaire, y compris les réponses ou les fils de commentaires. Il comprend également le numéro de ligne et	Le contenu du commentaire, numéro de ligne, ligne de code, ou tout fil de commentaires.

Service	Événement	L'option Total inclut	L'option Basique n'inclut pas
		la ligne de code sur laquelle le commentaire a été fait.	
CodeCommit	Demande d'extraction créée	Tous les détails de l'événement et le nombre de fichiers ajoutés, modifiés ou supprimés dans la demande d'extraction par rapport à la branche de destination.	Aucune liste de fichiers ni aucun détail indiquant si la branche source de la requête d'extraction a ajouté, modifié ou supprimé des fichiers.
CodePipeline	Approbation manuelle requise	Tous les détails de l'événement et les données personnalisées (si configurées). La notification comprend également un lien vers l'approbation requise dans le pipeline.	Pas de données personnalisées ou de lien.
CodePipeline	Échec de l'exécution de l'action Échec de l'exécution du pipeline Échec de l'exécution de la phase	Tous les détails de l'événement et le contenu du message d'erreur pour l'échec.	Pas de contenu du message d'erreur.

Cibles

Une cible est un emplacement où recevoir des notifications à partir de règles de notification. Les types de cible autorisés sont les rubriques Amazon SNS et les clients AWS Chatbot configurés pour les canaux Slack ou Microsoft Teams. Tout utilisateur abonné à la cible reçoit des notifications sur les événements que vous spécifiez dans la règle de notification.

Si vous souhaitez étendre la portée des notifications, vous pouvez configurer manuellement l'intégration entre les notifications et AWS Chatbot afin que les notifications soient envoyées aux salles de discussion Amazon Chime. Vous pouvez ensuite choisir la rubrique Amazon SNS configurée pour ce client AWS Chatbot comme cible de la règle de notification. Pour de plus amples informations, veuillez consulter Pour intégrer les notifications avec AWS Chatbot et Amazon Chime.

Si vous choisissez d'utiliser un client AWS Chatbot comme cible, vous devez d'abord créer ce client dans AWS Chatbot. Lorsque vous choisissez un client AWS Chatbot comme cible pour une règle de notification, une rubrique Amazon SNS est configurée pour ce client AWS Chatbot avec toutes les stratégies requises pour que les notifications soient envoyées au canal Slack ou Microsoft Teams. Vous n'avez pas à configurer les rubriques Amazon SNS existantes pour le client AWS Chatbot.

Vous pouvez choisir de créer une rubrique Amazon SNS en tant que cible dans le cadre de la création d'une règle de notification (recommandé). Vous pouvez également choisir une rubrique Amazon SNS existante dans la même région AWS que la règle de notification, mais vous devez la configurer avec la stratégie requise. La rubrique Amazon SNS que vous utilisez pour une cible doit se trouver dans votre compte AWS. Elle doit également se trouver dans la même région AWS que la règle de notification et la ressource AWS pour laquelle la règle a été créée.

Par exemple, si vous créez une règle de notification pour un référentiel dans la région USA Est (Ohio), la rubrique Amazon SNS doit également exister dans cette région. Si vous créez une rubrique Amazon SNS dans le cadre de la création d'une règle de notification, la rubrique est configurée avec la stratégie requise pour autoriser la publication d'événements dans la rubrique. C'est la meilleure méthode pour travailler avec des cibles et des règles de notification. Si vous choisissez d'utiliser une rubrique déjà existante ou d'en créer une manuellement, vous devez la configurer avec les autorisations requises avant que les utilisateurs ne reçoivent des notifications. Pour de plus amples informations, veuillez consulter Configurer une rubrique Amazon SNS pour les notifications.

> **Note**
>
> Si vous souhaitez utiliser une rubrique Amazon SNS existante au lieu d'en créer une nouvelle, dans Targets (Cibles), choisissez son ARN. Assurez-vous que la rubrique

dispose de la stratégie d'accès appropriée et que la liste d'abonnés contient uniquement les utilisateurs autorisés à voir des informations sur le pipeline. Si la rubrique Amazon SNS est une rubrique qui a été utilisée pour les notifications CodeCommit avant le 5 novembre 2019, elle contient une stratégie qui permet à CodeCommit publier sur cette rubrique et qui contient des autorisations différentes de celles requises pour AWS CodeStar Notifications. L'utilisation de ces rubriques n'est pas recommandée. Si vous souhaitez utiliser une rubrique créée pour cette expérience, vous devez ajouter la stratégie requise pour AWS CodeStar Notifications en plus de celle qui existe déjà. Pour plus d'informations, consultez Configurer une rubrique Amazon SNS pour les notifications et Présentation du contenu des notifications et de la sécurité.

Notifications et AWS CodeStar Notifications

Bien que ce soit une fonction de la console Outils pour développeurs, les notifications possèdent leur propre API, AWS CodeStar Notifications. Il a également son propre type de ressource AWS (règles de notification), ses autorisations et ses événements. Les événements des règles de notification sont enregistrés dans AWS CloudTrail. Les actions d'API peuvent être autorisées ou refusées via les stratégies IAM.

Événements pour les règles de notification sur les référentiels

Catégorie	Événements	ID d'événement

Commentaires	Sur les validations
	
	Sur les demandes d'extraction
		`codecommit-repository-comments-on-commits`
		
		`codecommit-repository-comments-on-pull-requests`

Approbations	Statut modifié
	
	Remplacement de la règle
		`codecommit-repository-approvals-status-changed`
		
		`codecommit-repository-approvals-rule-override`

Catégorie	Événements	ID d'événement

Demande d'extraction	Créé
	Source mise à jour
	Statut modifié
	Fusionnée
		`codecommit-repository-pull-request-created`
		`codecommit-repository-pull-request-source-updated`
		`codecommit-repository-pull-request-status-changed`
		`codecommit-repository-pull-request-merged`

Branches et balises	Créé
	Supprimé
	Mis à jour
		`codecommit-repository-branches-and-tags-created`
		`codecommit-repository-branches-and-tags-deleted`
		`codecommit-repository-branches-and-tags-updated`

Événements pour les règles de notification sur les projets de génération

Catégorie	Événements	ID d'événement
État de génération	Échec Réussi En cours Arrêté(e)	`codebuild-project-build-state-failed` `codebuild-project-build-state-succeeded`

Catégorie	Événements	ID d'événement
		`codebuild-project-build-state-in-progress` `codebuild-project-build-state-stopped`
Phase de génération	Échec Réussite	`codebuild-project-build-phase-failure` `codebuild-project-build-phase-success`

Événements pour les règles de notification sur les applications de déploiement

Catégorie	Événements	ID d'événement

Déploiement	Échec
	Réussi
	Démarré(e)
		`codedeploy-application-deployment-failed`
		`codedeploy-application-deployment-succeeded`
		`codedeploy-application-deployment-started`

Événements pour les règles de notification sur les pipelines

Catégorie	Événements	ID d'événement
Exécution de l'action	Réussi Échec Annulé Démarré(e)	`codepipeline-pipeline-action-execution-succeeded` `codepipeline-pipeline-action-execution-failed`

Catégorie	Événements	ID d'événement
		`codepipeline-pipeline-action-execution-canceled` `codepipeline-pipeline-action-execution-started`

Exécution de l'étape	Démarré(e)
	Réussi
	Reprise
	Annulé
	Échec
		`codepipeline-pipeline-stage-execution-started`
		`codepipeline-pipeline-stage-execution-succeeded`
		`codepipeline-pipeline-stage-execution-resumed`
		`codepipeline-pipeline-stage-execution-canceled`
		`codepipeline-pipeline-stage-execution-failed`

Exécution du pipeline	Échec
	Annulé
	Démarré(e)
	Reprise
	Réussi
	Remplacé
		`codepipeline-pipeline-pipeline-execution-failed`
		`codepipeline-pipeline-pipeline-execution-canceled`
		`codepipeline-pipeline-pipeline-execution-started`
		`codepipeline-pipeline-pipeline-execution-resumed`
		`codepipeline-pipeline-pipeline-execution-succeeded`
		`codepipeline-pipeline-pipeline-execution-superseded`

Catégorie	Événements	ID d'événement

Approbation manuelle	Échec
	
	Nécessaire
	
	Réussi
		`codepipeline-pipeline-manual-approval-failed`
		
		`codepipeline-pipeline-manual-approval-needed`
		`codepipeline-pipeline-manual-approval-succeeded`

Configuration

Si vous disposez d'une stratégie gérée pour AWS CodeBuild, AWS CodeCommit, AWS CodeDeploy ou AWS CodePipeline appliquée à votre utilisateur ou rôle IAM, vous disposez des autorisations requises pour utiliser les notifications dans les limites des rôles et autorisations fournis par la stratégie. Par exemple, les utilisateurs auxquels la stratégie `AWSCodeBuildAdminAccess`, `AWSCodeCommitFullAccess`, `AWSCodeDeployFullAccess` ou `AWSCodePipeline_FullAccess` gérée est appliquée disposent d'un accès administratif complet aux notifications.

Pour plus d'informations, y compris des exemples de stratégie, consultez Politiques basées sur l'identité.

Si l'une de ces stratégies est appliquée à votre utilisateur ou rôle IAM, et qu'un projet de construction dans CodeBuild, un référentiel dans CodeCommit, une application de déploiement dans CodeDeploy ou un pipeline dans CodePipeline, vous êtes prêt à créer votre première règle de notification. Passez au Prise en main des notifications. Dans le cas contraire, consultez les rubriques suivantes :

- CodeBuild : Mise en route avec CodeBuild
- CodeCommit :Mise en route avec CodeCommit
- CodeDeploy :Didacticiels
- CodePipeline :Mise en route avec CodePipeline

Si vous souhaitez gérer vous-même les autorisations administratives pour les notifications pour les utilisateurs, les groupes ou les rôles IAM, suivez les procédures de cette rubrique pour configurer les autorisations et les ressources dont vous avez besoin pour utiliser le service.

Si vous souhaitez utiliser des rubriques Amazon SNS précédemment créées pour les notifications au lieu de créer des rubriques spécifiquement pour les notifications, vous devez configurer une rubrique Amazon SNS à utiliser comme cible pour une règle de notification en appliquant une stratégie qui autorise la publication d'événements sur cette rubrique.

> **Note**
>
> Pour effectuer les procédures suivantes, vous devez être connecté avec un compte disposant d'autorisations administratives. Pour plus d'informations, consultez la section Création de votre premier utilisateur administrateur et groupe IAM.

Rubriques

- Créer et appliquer une stratégie pour l'accès administratif aux notifications
- Configurer une rubrique Amazon SNS pour les notifications
- Abonner les utilisateurs aux rubriques Amazon SNS qui sont des cibles

Créer et appliquer une stratégie pour l'accès administratif aux notifications

Vous pouvez administrer les notifications en vous connectant avec un utilisateur IAM ou en utilisant un rôle disposant d'autorisations pour accéder au service et aux services (AWS CodeBuild, AWS CodeCommit, AWS CodeDeploy ou AWS CodePipeline) pour lesquels vous souhaitez créer des notifications. Vous pouvez également créer vos propres stratégies et les appliquer à des utilisateurs ou à des groupes.

La procédure suivante vous montre comment configurer un groupe IAM avec des autorisations pour l'administration des notifications et l'ajout d'utilisateurs IAM. Si vous ne souhaitez pas configurer un groupe, vous pouvez appliquer cette stratégie directement aux utilisateurs iAM ou à un rôle IAM qui peut être assumé par les utilisateurs. Vous pouvez également utiliser les stratégies gérées pour CodeBuild, CodeCommit, CodeDeploy ou CodePipeline, qui incluent un accès approprié aux fonctionnalités de notification en fonction de l'étendue de la stratégie.

Pour la politique ci-dessous, entrez un nom (par exemple, `AWSCodeStarNotificationsFullAccess`) et une description facultative pour cette politique. La description vous aide à vous souvenir de l'objectif de cette politique (par exemple, **`This policy provides full access to AWS CodeStar Notifications.`**)

Pour utiliser l'éditeur de politique JSON afin de créer une politique

1. Connectez-vous à la AWS Management Console et ouvrez la console IAM à l'adresse https://console.aws.amazon.com/iam/.
2. Dans le panneau de navigation de gauche, sélectionnez Policies (Politiques).

   Si vous sélectionnez Politiques pour la première fois, la page Bienvenue dans les politiques gérées s'affiche. Sélectionnez Mise en route.
3. En haut de la page, sélectionnez Créer une politique.
4. Dans la section Éditeur de politiques, choisissez l'option JSON.
5. Entrez le document de politique JSON suivant :

```
{
   "Version": "2012-10-17",
   "Statement": [
     {
       "Sid": "AWSCodeStarNotificationsFullAccess",
       "Effect": "Allow",
       "Action": [
           "codestar-notifications:CreateNotificationRule",
           "codestar-notifications:DeleteNotificationRule",
           "codestar-notifications:DescribeNotificationRule",
           "codestar-notifications:ListNotificationRules",
           "codestar-notifications:UpdateNotificationRule",
           "codestar-notifications:Subscribe",
           "codestar-notifications:Unsubscribe",
           "codestar-notifications:DeleteTarget",
           "codestar-notifications:ListTargets",
           "codestar-notifications:ListTagsforResource",
           "codestar-notifications:TagResource",
           "codestar-notifications:UntagResource"
       ],
       "Resource": "*"
     }
   ]
}
```

6. Choisissez Next (Suivant).

> **Note**
>
> Vous pouvez basculer à tout moment entre les options des éditeurs visuel et JSON. Toutefois, si vous apportez des modifications ou si vous choisissez Suivant dans l'éditeur visuel, IAM peut restructurer votre politique afin de l'optimiser pour l'éditeur visuel. Pour de plus amples informations, consulte Restructuration d'une politique dans le Guide de l'utilisateur IAM.

7. Sur la page Vérifier et créer, saisissez un Nom de politique et une Description (facultative) pour la politique que vous créez. Vérifiez les Autorisations définies dans cette politique pour voir les autorisations accordées par votre politique.
8. Choisissez Create policy (Créer une politique) pour enregistrer votre nouvelle politique.

Configurer une rubrique Amazon SNS pour les notifications

Le moyen le plus simple de configurer des notifications consiste à créer une rubrique Amazon SNS lorsque vous créez une règle de notification. Vous pouvez utiliser une rubrique Amazon SNS existante si elle répond aux exigences suivantes :

- Elle a été créée dans la même Région AWS que la ressource (projet de génération, application de déploiement, référentiel ou pipeline) pour laquelle vous souhaitez créer des règles de notification.
- Elle n'a pas été utilisée pour l'envoi de notifications pour CodeCommit avant le 5 novembre 2019. Si c'est le cas, elle contiendra les déclarations de stratégie qui ont activé cette fonctionnalité. Vous pouvez choisir d'utiliser cette rubrique, mais vous devrez ajouter la stratégie supplémentaire comme indiqué dans la procédure. Vous ne devez pas supprimer la déclaration de stratégie existante si un ou plusieurs référentiels sont toujours configurés pour les notifications avant le 5 novembre 2019.
- Elle comporte une stratégie qui autorise AWS CodeStar Notifications à publier des notifications dans la rubrique.

Pour créer une rubrique Amazon SNS à utiliser comme cible pour les règles AWS CodeStar Notifications

1. Connectez-vous à AWS Management Console et ouvrez la console Amazon SNS à l'adresse https://console.aws.amazon.com/sns/v3/home.

2. Dans la barre de navigation, choisissez Rubriques, choisissez la rubrique à configurer, puis Modifier.
3. Développer Access policy (Stratégie d'accès), puis choisissez Advanced (Avancé).
4. Dans l'éditeur JSON, ajoutez la déclaration suivante à la stratégie. Inclure l'ARN de la rubrique, Région AWS, l'ID Compte AWS et le nom de la rubrique.

```
 {
      "Sid": "AWSCodeStarNotifications_publish",
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "codestar-notifications.amazonaws.com"
        ]
      },
      "Action": "SNS:Publish",
      "Resource": "arn:aws:sns:us-east-2:123456789012:codestar-notifications-
MyTopicForNotificationRules"
    }
```

Cette déclaration de stratégie doit ressembler à l'exemple suivant.

```
{
  "Version": "2008-10-17",
  "Id": "__default_policy_ID",
  "Statement": [
    {
      "Sid": "__default_statement_ID",
      "Effect": "Allow",
      "Principal": {
        "AWS": "*"
      },
      "Action": [
        "SNS:GetTopicAttributes",
        "SNS:SetTopicAttributes",
        "SNS:AddPermission",
        "SNS:RemovePermission",
        "SNS:DeleteTopic",
        "SNS:Subscribe",
        "SNS:ListSubscriptionsByTopic",
        "SNS:Publish",
        "SNS:Receive"
```

```
      ],
      "Resource": "arn:aws:sns:us-east-2:123456789012:codestar-notifications-
MyTopicForNotificationRules",
      "Condition": {
        "StringEquals": {
          "AWS:SourceOwner": "123456789012"
        }
      }
    },
 {
      "Sid": "AWSCodeStarNotifications_publish",
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "codestar-notifications.amazonaws.com"
        ]
      },
      "Action": "SNS:Publish",
      "Resource": "arn:aws:sns:us-east-2:123456789012:codestar-notifications-
MyTopicForNotificationRules"
    }
  ]
}
```

5. Sélectionnez Save Changes (Enregistrer les modifications).
6. Si vous souhaitez utiliser une rubrique Amazon SNS chiffrée AWS KMS pour envoyer des notifications, vous devez également activer la compatibilité entre la source d'événement (AWS CodeStar Notifications) et la rubrique chiffrée en ajoutant l'instruction suivante à la stratégie de AWS KMS key. Remplacez la Région AWS (dans cet exemple, us-east-2) par la Région AWS dans laquelle la clé a été créée.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "codestar-notifications.amazonaws.com"
            },
            "Action": [
                "kms:GenerateDataKey*",
                "kms:Decrypt"
```

```
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "kms:ViaService": "sns.us-east-2.amazonaws.com"
                }
            }
        }
    ]
}
```

Pour plus d'informations, consultez Chiffrement au repos et Utilisation des conditions de stratégie avec AWS KMS dans le Guide du développeur AWS Key Management Service.

Abonner les utilisateurs aux rubriques Amazon SNS qui sont des cibles

Avant que les utilisateurs puissent recevoir des notifications, ils doivent être abonnés à la rubrique Amazon SNS cible de la règle de notification. Si les utilisateurs sont abonnés par adresse e-mail, ils doivent confirmer leur abonnement avant de recevoir des notifications. Pour envoyer des notifications aux utilisateurs dans des canaux Slack, des canaux Microsoft Teams ou des salles de conversation Amazon Chime, consultez Configurer l'intégration entre les notifications et AWS Chatbot.

Pour abonner les utilisateurs à une rubrique Amazon SNS utilisée pour les notifications

1. Connectez-vous à AWS Management Console et ouvrez la console Amazon SNS à l'adresse https://console.aws.amazon.com/sns/v3/home.
2. Dans le panneau de navigation, choisissez Topics (Rubriques), puis choisissez la rubrique à laquelle vous voulez abonner les utilisateurs.
3. Dans Subscriptions (Abonnements), choisissez Create subscription (Créer un abonnement).
4. Dans Protocole, choisissez E-mail. Dans Point de terminaison, saisissez votre adresse e-mail, puis choisissez Créer un abonnement.

Prise en main des notifications

La façon la plus simple de commencer à utiliser les notifications consiste à configurer une règle de notification sur l'un de vos projets de construction, applications de déploiement, pipelines ou référentiels.

> **Note**
>
> La première fois que vous créez une règle de notification, un rôle lié à un service est créé dans votre compte. Pour de plus amples informations, veuillez consulter Utilisation de rôles liés à un service pour AWS CodeStar Notifications.

Rubriques

Prérequis

Suivez les étapes de Configuration. Vous avez également besoin d'une ressource pour laquelle vous créez une règle de notification.

- Créez un projet de génération dans CodeBuild ou utilisez un projet existant.
- Créez une application ou utilisez une application de déploiement existante.
- Créez un pipeline dans CodePipeline ou utilisez un pipeline existant.
- Créez un référentiel AWS CodeCommit ou utilisez un référentiel existant.

Création d'une règle de notification pour un référentiel

Vous pouvez créer des règles de notification pour envoyer des notifications sur les événements de votre référentiel qui sont importants pour vous. Les étapes suivantes vous montrent comment configurer une règle de notification sur un seul événement de référentiel. Ces étapes sont écrites en supposant que vous avez un référentiel configuré dans votre compte AWS.

> **Important**
>
> Si vous avez configuré des notifications dans CodeCommit avant le 5 novembre 2019, les rubriques Amazon SNS utilisées pour ces notifications contiennent une stratégie qui permet

à CodeCommit publier sur cette rubrique et qui contient des autorisations différentes de celles requises pour AWS CodeStar Notifications. L'utilisation de ces rubriques n'est pas recommandée. Si vous souhaitez utiliser une rubrique créée pour cette expérience, vous devez ajouter la stratégie requise pour AWS CodeStar Notifications en plus de celle qui existe déjà. Pour plus d'informations, consultez Configurer une rubrique Amazon SNS pour les notifications et Présentation du contenu des notifications et de la sécurité.

1. Ouvrez la console CodeCommit, à l'adresse https://console.aws.amazon.com/codecommit/.
2. Choisissez un référentiel dans la liste et ouvrez-le.
3. Choisissez Notify (Notifier), puis Create notification rule (Créer une règle de notification). Vous pouvez également choisir Paramètres, Notifications, puis Créer une règle de notification.
4. Dans Notification name (Nom de la notification), saisissez le nom de la règle.
5. Dans Detail type (Type de détail), choisissez Basic (Basique) si vous souhaitez que seules les informations fournies à Amazon EventBridge soient incluses dans la notification. Choisissez Full (Complète), si vous souhaitez inclure dans la notification les informations fournies à Amazon EventBridge et celles qui peuvent être fournies par le service de ressource ou le gestionnaire de notifications.

   Pour de plus amples informations, veuillez consulter Présentation du contenu des notifications et de la sécurité.
6. Dans Événements qui déclenchent des notifications, sous Branches et balises, sélectionnez Créé.
7. Dans Targets (Cibles), choisissez Create SNS topic (Créer une rubrique SNS).

   > **Note**
   >
   > Lorsque vous créez la rubrique dans le cadre de la création de la règle de notification, la stratégie qui permet à CodeCommit de publier des événements dans la rubrique est appliquée automatiquement. L'utilisation d'une rubrique créée pour les règles de notification vous permet de vous assurer que vous n'abonnez que les utilisateurs pour lesquels vous souhaitez qu'ils reçoivent des notifications sur ce référentiel.

   Après le préfixe codestar-notifications-, entrez un nom pour la rubrique, puis choisissez Submit (Envoyer).

> **Note**
>
> Si vous souhaitez utiliser une rubrique Amazon SNS existante au lieu d'en créer une nouvelle, dans Targets (Cibles), choisissez son ARN. Assurez-vous que la rubrique dispose de la stratégie d'accès appropriée et que la liste d'abonnés contient uniquement les utilisateurs autorisés à voir des informations sur le pipeline. Si la rubrique Amazon SNS est une rubrique qui a été utilisée pour les notifications CodeCommit avant le 5 novembre 2019, elle contient une stratégie qui permet à CodeCommit publier sur cette rubrique et qui contient des autorisations différentes de celles requises pour AWS CodeStar Notifications. L'utilisation de ces rubriques n'est pas recommandée. Si vous souhaitez utiliser une rubrique créée pour cette expérience, vous devez ajouter la stratégie requise pour AWS CodeStar Notifications en plus de celle qui existe déjà. Pour plus d'informations, consultez Configurer une rubrique Amazon SNS pour les notifications et Présentation du contenu des notifications et de la sécurité.

8. Choisissez Submit (Envoyer), puis passez en revue la règle de notification créée.
9. Abonnez votre adresse e-mail à la rubrique Amazon SNS que vous venez de créer. Pour de plus amples informations, veuillez consulter Pour abonner les utilisateurs à une rubrique Amazon SNS utilisée pour les notifications.
10. Accédez à votre référentiel et créez une branche de test à partir de la branche par défaut.
11. Après avoir créé la branche, la règle de notification envoie une notification à tous les abonnés de rubrique contenant des informations sur cet événement.

Création d'une règle de notification pour un projet de génération

Vous pouvez créer des règles de notification pour envoyer des notifications sur les événements de votre projet de génération qui sont importants pour vous. Les étapes suivantes vous montrent comment configurer une règle de notification sur un seul événement de projet de génération. Ces étapes sont écrites en supposant que vous avez un projet de build configuré dans votre compte AWS.

1. Ouvrez la console CodeBuild à l'adresse.https://console.aws.amazon.com/codebuild/.
2. Choisissez un projet de build dans la liste et ouvrez-le.

3. Choisissez Notify (Notifier), puis Create notification rule (Créer une règle de notification). Vous pouvez également choisir Settings (Paramètres), puis Create notification rule (Créer une règle de notification).
4. Dans Notification name (Nom de la notification), saisissez le nom de la règle.
5. Dans Detail type (Type de détail), choisissez Basic (Basique) si vous souhaitez que seules les informations fournies à Amazon EventBridge soient incluses dans la notification. Choisissez Full (Complète), si vous souhaitez inclure dans la notification les informations fournies à Amazon EventBridge et celles qui peuvent être fournies par le service de ressource ou le gestionnaire de notifications.

   Pour de plus amples informations, veuillez consulter Présentation du contenu des notifications et de la sécurité.
6. Dans Événements qui déclenchent des notifications, sous Phase de génération, sélectionnez Succès.
7. Dans Targets (Cibles), choisissez Create SNS topic (Créer une rubrique SNS).

   > **Note**
   >
   > Lorsque vous créez la rubrique dans le cadre de la création de la règle de notification, la stratégie qui permet à CodeBuild de publier des événements dans la rubrique est appliquée automatiquement. L'utilisation d'une rubrique créée pour les règles de notification vous permet de vous assurer que vous n'abonnez que les utilisateurs pour lesquels vous souhaitez qu'ils reçoivent des notifications sur ce projet de build.

   Après le préfixe codestar-notifications- entrez un nom pour la rubrique, puis choisissez Submit (Envoyer).

   > **Note**
   >
   > Si vous souhaitez utiliser une rubrique Amazon SNS existante au lieu d'en créer une nouvelle, dans Targets (Cibles), choisissez son ARN. Assurez-vous que la rubrique dispose de la stratégie d'accès appropriée et que la liste d'abonnés contient uniquement les utilisateurs autorisés à voir des informations sur le pipeline. Si la rubrique Amazon SNS est une rubrique qui a été utilisée pour les notifications CodeCommit avant le 5 novembre 2019, elle contient une stratégie qui permet à CodeCommit publier sur

cette rubrique et qui contient des autorisations différentes de celles requises pour AWS CodeStar Notifications. L'utilisation de ces rubriques n'est pas recommandée. Si vous souhaitez utiliser une rubrique créée pour cette expérience, vous devez ajouter la stratégie requise pour AWS CodeStar Notifications en plus de celle qui existe déjà. Pour plus d'informations, consultez Configurer une rubrique Amazon SNS pour les notifications et Présentation du contenu des notifications et de la sécurité.

8. Choisissez Submit (Envoyer), puis passez en revue la règle de notification créée.
9. Abonnez votre adresse e-mail à la rubrique Amazon SNS que vous venez de créer. Pour de plus amples informations, veuillez consulter Pour abonner les utilisateurs à une rubrique Amazon SNS utilisée pour les notifications.
10. Accédez à votre projet de génération et démarrez une génération.
11. Une fois la phase de construction terminée, la règle de notification envoie une notification à tous les abonnés de rubrique contenant des informations sur cet événement.

Créer une règle de notification pour une application de déploiement

Vous pouvez créer des règles de notification pour envoyer des notifications sur les événements de votre application de déploiement qui sont importants pour vous. Les étapes suivantes vous montrent comment configurer une règle de notification sur un seul événement de projet de génération. Ces étapes sont écrites en supposant que vous avez une application de déploiement configurée dans votre compte AWS.

1. Ouvrez la console CodeDeploy à l'adresse https://console.aws.amazon.com/codedeploy/.
2. Choisissez une application dans la liste et ouvrez-la.
3. Choisissez Notify (Notifier), puis Create notification rule (Créer une règle de notification). Vous pouvez également choisir Settings (Paramètres), puis Create notification rule (Créer une règle de notification).
4. Dans Notification name (Nom de la notification), saisissez le nom de la règle.
5. Dans Detail type (Type de détail), choisissez Basic (Basique) si vous souhaitez que seules les informations fournies à Amazon EventBridge soient incluses dans la notification. Choisissez Full (Complète), si vous souhaitez inclure dans la notification les informations fournies à Amazon EventBridge et celles qui peuvent être fournies par le service de ressource ou le gestionnaire de notifications.

Pour de plus amples informations, veuillez consulter Présentation du contenu des notifications et de la sécurité.

6. Dans Événements qui déclenchent des notifications, sous Déploiement, sélectionnez Succès.
7. Dans Targets (Cibles), choisissez Create SNS topic (Créer une rubrique SNS).

> **Note**
>
> Lorsque vous créez la rubrique dans le cadre de la création de la règle de notification, la stratégie qui permet à CodeDeploy de publier des événements dans la rubrique est appliquée automatiquement. L'utilisation d'une rubrique créée pour les règles de notification vous permet de vous assurer que vous n'abonnez que les utilisateurs pour lesquels vous souhaitez qu'ils reçoivent des notifications sur cette application de déploiement.

Après le préfixe codestar-notifications- entrez un nom pour la rubrique, puis choisissez Submit (Envoyer).

> **Note**
>
> Si vous souhaitez utiliser une rubrique Amazon SNS existante au lieu d'en créer une nouvelle, dans Targets (Cibles), choisissez son ARN. Assurez-vous que la rubrique dispose de la stratégie d'accès appropriée et que la liste d'abonnés contient uniquement les utilisateurs autorisés à voir des informations sur le pipeline. Si la rubrique Amazon SNS est une rubrique qui a été utilisée pour les notifications CodeCommit avant le 5 novembre 2019, elle contient une stratégie qui permet à CodeCommit publier sur cette rubrique et qui contient des autorisations différentes de celles requises pour AWS CodeStar Notifications. L'utilisation de ces rubriques n'est pas recommandée. Si vous souhaitez utiliser une rubrique créée pour cette expérience, vous devez ajouter la stratégie requise pour AWS CodeStar Notifications en plus de celle qui existe déjà. Pour plus d'informations, consultez Configurer une rubrique Amazon SNS pour les notifications et Présentation du contenu des notifications et de la sécurité.

8. Choisissez Submit (Envoyer), puis passez en revue la règle de notification créée.

9. Abonnez votre adresse e-mail à la rubrique Amazon SNS que vous venez de créer. Pour de plus amples informations, veuillez consulter Pour abonner les utilisateurs à une rubrique Amazon SNS utilisée pour les notifications.
10. Accédez à votre application de déploiement et démarrez un déploiement.
11. Une fois le déploiement réussi, la règle de notification envoie une notification à tous les abonnés du sujet avec des informations sur l'événement.

Création d'une règle de notification pour un pipeline

Vous pouvez créer des règles de notification pour envoyer des notifications sur les événements de votre pipeline qui sont importants pour vous. Les étapes suivantes vous montrent comment configurer une règle de notification sur un seul événement de pipeline. Ces étapes sont écrites en supposant que vous avez un pipeline configuré dans votre compte AWS.

1. Ouvrez la console CodePipeline à l'adresse https://console.aws.amazon.com/codepipeline/.
2. Choisissez un pipeline dans la liste et ouvrez-le.
3. Choisissez Notify (Notifier), puis Create notification rule (Créer une règle de notification). Vous pouvez également choisir Settings (Paramètres), puis Create notification rule (Créer une règle de notification).
4. Dans Notification name (Nom de la notification), saisissez le nom de la règle.
5. Dans Detail type (Type de détail), choisissez Basic (Basique) si vous souhaitez que seules les informations fournies à Amazon EventBridge soient incluses dans la notification. Choisissez Full (Complète), si vous souhaitez inclure dans la notification les informations fournies à Amazon EventBridge et celles qui peuvent être fournies par le service de ressource ou le gestionnaire de notifications.

   Pour de plus amples informations, veuillez consulter Présentation du contenu des notifications et de la sécurité.
6. Dans Événements qui déclenchent des notifications, sous Exécution de l'action, sélectionnez Démarré.
7. Dans Targets (Cibles), choisissez Create SNS topic (Créer une rubrique SNS).

> **Note**
>
> Lorsque vous créez la rubrique dans le cadre de la création de la règle de notification, la stratégie qui permet à CodePipeline de publier des événements dans la rubrique

est appliquée automatiquement. L'utilisation d'une rubrique créée pour les règles de notification vous permet de vous assurer que vous n'abonnez que les utilisateurs pour lesquels vous souhaitez qu'ils reçoivent des notifications sur ce pipeline.

Après le préfixe codestar-notifications-, entrez un nom pour la rubrique, puis choisissez Submit (Envoyer).

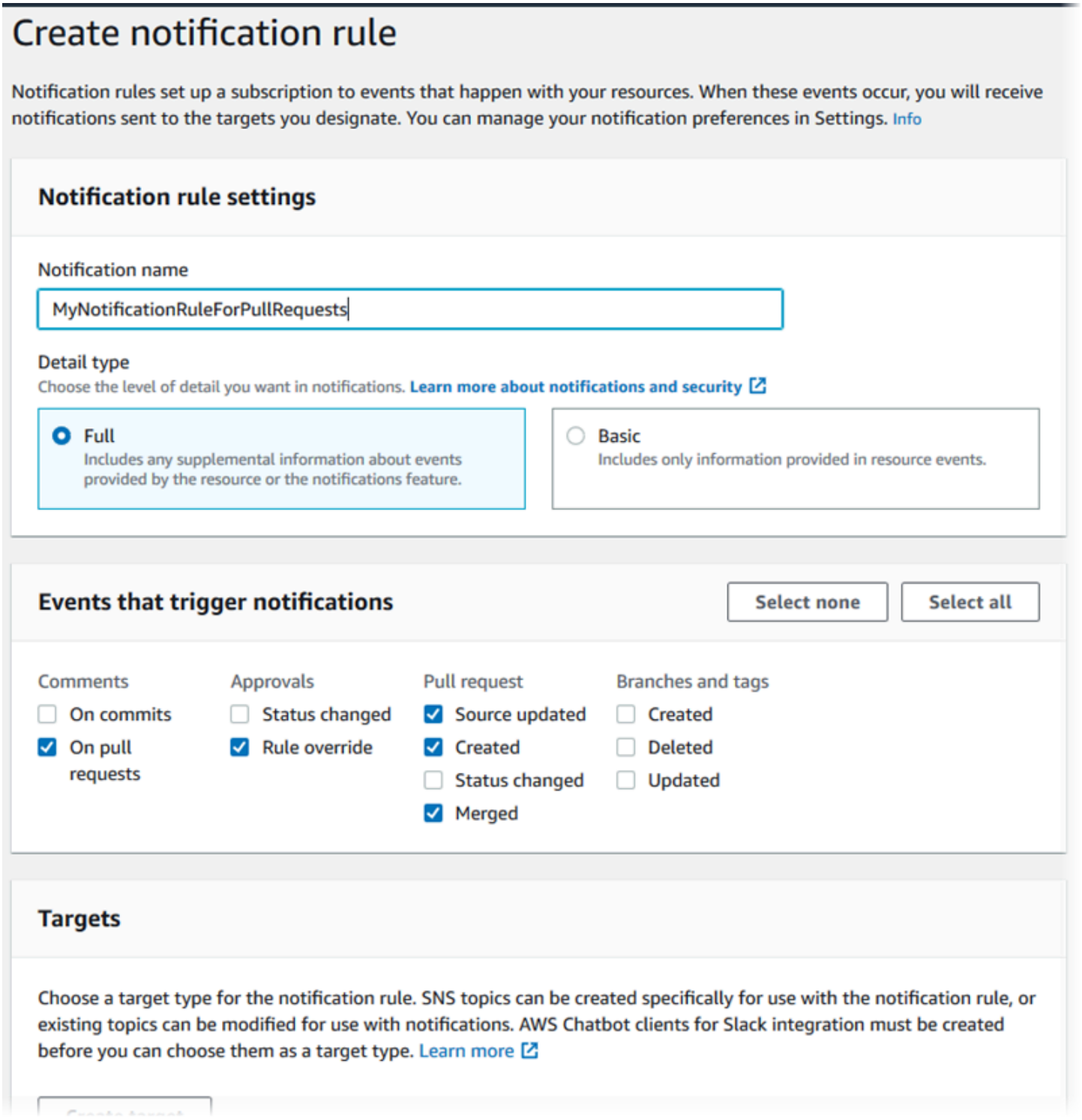
> **Note**
>
> Si vous souhaitez utiliser une rubrique Amazon SNS existante au lieu d'en créer une nouvelle, dans Targets (Cibles), choisissez son ARN. Assurez-vous que la rubrique dispose de la stratégie d'accès appropriée et que la liste d'abonnés contient uniquement les utilisateurs autorisés à voir des informations sur le pipeline. Si la rubrique Amazon SNS est une rubrique qui a été utilisée pour les notifications CodeCommit avant le 5 novembre 2019, elle contient une stratégie qui permet à CodeCommit publier sur cette rubrique et qui contient des autorisations différentes de celles requises pour AWS CodeStar Notifications. L'utilisation de ces rubriques n'est pas recommandée. Si vous souhaitez utiliser une rubrique créée pour cette expérience, vous devez ajouter la stratégie requise pour AWS CodeStar Notifications en plus de celle qui existe déjà. Pour plus d'informations, consultez Configurer une rubrique Amazon SNS pour les notifications et Présentation du contenu des notifications et de la sécurité.

8. Choisissez Submit (Envoyer), puis passez en revue la règle de notification créée.
9. Abonnez votre adresse e-mail à la rubrique Amazon SNS que vous venez de créer. Pour de plus amples informations, veuillez consulter Pour abonner les utilisateurs à une rubrique Amazon SNS utilisée pour les notifications.
10. Accédez à votre pipeline, puis choisissez Release change (Changement de version).
11. Lorsque l'action démarre, la règle de notification envoie une notification à tous les abonnés de la rubrique, contenant les informations sur l'événement.

Utilisation des règles de notification

C'est l'endroit où vous configurez les événements pour lesquels vous voulez que les utilisateurs reçoivent des notifications et spécifiez les cibles qui recevront ces notifications. Vous pouvez envoyer des notifications directement aux utilisateurs via Amazon SNS ou via des clients AWS Chatbot

configurés pour les canaux Slack ou Microsoft Teams. Si vous souhaitez étendre la portée des notifications, vous pouvez configurer manuellement l'intégration entre les notifications et AWS Chatbot afin que les notifications soient envoyées aux salles de discussion Amazon Chime. Pour plus d'informations, consultez Cibles et Pour intégrer les notifications avec AWS Chatbot et Amazon Chime.



Vous pouvez utiliser la console Outils pour développeurs ou la AWS CLI pour créer et gérer des règles de notification.

Rubriques

Création d'une règle de notification

Vous pouvez utiliser la console Outils pour développeurs ou la AWS CLI pour créer des règles de notification. Vous pouvez créer une rubrique Amazon SNS à utiliser comme cible d'une règle de notification dans le cadre de la création de la règle. Si vous souhaitez utiliser un client AWS Chatbot comme cible, vous devez créer ce client pour pouvoir créer la règle. Pour de plus amples informations, veuillez consulter Configurer un client AWS Chatbot pour un canal Slack.

Pour créer une règle de notification (console)

1. Ouvrez la console Outils pour développeurs AWS à l'adresse https://console.aws.amazon.com/codesuite/settings/notifications.
2. Utilisez la barre de navigation pour accéder à la ressource.
   - Pour CodeBuild, choisissez Build (Génération), Build projects (Projets de génération), puis choisissez un projet de génération.
   - Pour CodeCommit, choisissez Source, Repositories (Référentiels), puis choisissez un référentiel.
   - Pour CodeDeploy, choisissez Applications, puis sélectionnez une application.
   - Pour CodePipeline, choisissez Pipeline, Pipelines, puis choisissez un pipeline.
3. Sur la page des ressources, choisissez Notify (Notifier), puis Create notification rule (Créer une règle de notification). Vous pouvez également accéder à la page Settings (Paramètres) de la ressource, accéder à Notifications ou Notification rules (Règles de notification), puis choisir Create notification rule (Créer une règle de notification).
4. Dans Notification name (Nom de la notification), saisissez le nom de la règle.

5. Dans Detail type (Type de détail), choisissez Basic (Basique) si vous souhaitez que seules les informations fournies à Amazon EventBridge soient incluses dans la notification. Choisissez Full (Complète), si vous souhaitez inclure dans la notification les informations fournies à Amazon EventBridge et celles qui peuvent être fournies par le service de ressource ou le gestionnaire de notifications.

   Pour de plus amples informations, veuillez consulter Présentation du contenu des notifications et de la sécurité.

6. Dans Événements qui déclenchent des notifications, sélectionnez les événements pour lesquels vous souhaitez envoyer des notifications. Pour les types d'événement d'une ressource, veuillez consulter les rubriques suivantes :

   - CodeBuild : Événements pour les règles de notification sur les projets de génération
   - CodeCommit : Événements pour les règles de notification sur les référentiels
   - CodeDeploy : Événements pour les règles de notification sur les applications de déploiement
   - CodePipeline : Événements pour les règles de notification sur les pipelines

7. Dans Targets (Cibles), effectuez l'une des actions suivantes :

   - Si vous avez déjà configuré une ressource à utiliser avec les notifications, dans Choisir un type de cible, choisissez AWS Chatbot (Slack), AWS Chatbot (Microsoft Teams) ou Rubrique SNS. Dans Choisir une cible, choisissez le nom du client (pour un client Slack ou Microsoft Teams configuré dans AWS Chatbot) ou l'Amazon Resource Name (ARN) de la rubrique Amazon SNS (pour les rubriques Amazon SNS déjà configurées avec la politique requise pour les notifications).
   - Si vous n'avez pas configuré de ressource à utiliser avec les notifications, choisissez Create target (Créer une cible), puis SNS topic (Rubrique SNS). Donnez un nom à la rubrique après codestar-notifications-, puis choisissez Create (Créer).

> **Note**
>
> - Si vous créez la rubrique Amazon SNS dans le cadre de la création de la règle de notification, la stratégie qui permet à la fonctionnalité de notifications de publier des événements dans la rubrique est appliquée automatiquement. L'utilisation d'une rubrique créée pour les règles de notification vous permet de vous assurer que vous n'abonnez que les utilisateurs qui doivent recevoir des notifications sur ce référentiel.

- Vous ne pouvez pas créer un client AWS Chatbot dans le cadre de la création d'une règle de notification. Si vous choisissez AWS Chatbot (Slack) ou AWS Chatbot (Microsoft Teams), vous verrez un bouton vous demandant de configurer un client dans AWS Chatbot. Le choix de cette option provoque l'ouverture de la console AWS Chatbot. Pour de plus amples informations, veuillez consulter Configurer un client AWS Chatbot pour un canal Slack.
- Si vous souhaitez utiliser une rubrique Amazon SNS existante en tant que cible, vous devez ajouter la stratégie requise pour AWS CodeStar Notifications, en plus de toute autre stratégie qui pourrait exister pour cette rubrique. Pour plus d'informations, consultez Configurer une rubrique Amazon SNS pour les notifications et Présentation du contenu des notifications et de la sécurité.

8. Choisissez Submit (Envoyer), puis passez en revue la règle de notification créée.

> **Note**
>
> Les utilisateurs doivent s'abonner et confirmer leurs abonnements à la rubrique Amazon SNS que vous avez spécifiée comme cible de la règle avant de recevoir des notifications. Pour de plus amples informations, veuillez consulter Pour abonner les utilisateurs à une rubrique Amazon SNS utilisée pour les notifications.

Pour créer une règle de notification (AWS CLI)

1. À partir d'un terminal ou d'une invite de commandes, exécutez la commande create-notification rule pour générer le squelette JSON.

```
aws codestar-notifications create-notification-rule --generate-cli-skeleton
 > rule.json
```

   Vous pouvez donner au fichier le nom de votre choix. Dans cet exemple, le fichier est nommé *rule.json*.

2. Ouvrez le fichier JSON dans un éditeur de texte brut et modifiez-le pour y inclure la ressource, les types d'événements et la cible Amazon SNS souhaités pour la règle.

L'exemple suivant montre une règle de notification nommée **MyNotificationRule** pour un référentiel nommé *MyDemoRepo* dans un compte AWS avec l'ID *123456789012*. Les notifications avec le type de détail complet sont envoyées à une rubrique Amazon SNS nommée *MyNotificationTopic* lorsque les branches et les balises sont créées.

```
{
    "Name": "MyNotificationRule",
    "EventTypeIds": [
        "codecommit-repository-branches-and-tags-created"
    ],
    "Resource": "arn:aws:codecommit:us-east-1:123456789012:MyDemoRepo",
    "Targets": [
        {
            "TargetType": "SNS",
            "TargetAddress": "arn:aws:sns:us-
east-1:123456789012:MyNotificationTopic"
        }
    ],
    "Status": "ENABLED",
    "DetailType": "FULL"
}
```

Sauvegardez le fichier.

3. À l'aide du fichier que vous venez de modifier, à partir du terminal ou de la ligne de commande, exécutez à nouveau la commande create-notification-rule pour créer la règle de notification.

```
aws codestar-notifications create-notification-rule --cli-input-json
 file://rule.json
```

4. En cas de réussite, la commande renvoie l'ARN de la règle de notification, comme suit :

```
{
    "Arn": "arn:aws:codestar-notifications:us-east-1:123456789012:notificationrule/
dc82df7a-EXAMPLE"
}
```

Pour répertorier les types d'événement pour les règles de notification (AWS CLI)

1. À partir d'un terminal ou d'une invite de commande, exécutez la commande list-event-types. Vous pouvez utiliser l'option `--filters` pour limiter la réponse à un type de ressource spécifique ou à un autre attribut. Par exemple, la commande suivante renvoie une liste de types d'événements pour les applications CodeDeploy.

```
aws codestar-notifications list-event-types --filters
 Name=SERVICE_NAME,Value=CodeDeploy
```

2. Le résultat produit lors de l'exécution de cette commande est semblable à ce qui suit :

```
{
    "EventTypes": [
        {
            "EventTypeId": "codedeploy-application-deployment-succeeded",
            "ServiceName": "CodeDeploy",
            "EventTypeName": "Deployment: Succeeded",
            "ResourceType": "Application"
        },
        {
            "EventTypeId": "codedeploy-application-deployment-failed",
            "ServiceName": "CodeDeploy",
            "EventTypeName": "Deployment: Failed",
            "ResourceType": "Application"
        },
        {
            "EventTypeId": "codedeploy-application-deployment-started",
            "ServiceName": "CodeDeploy",
            "EventTypeName": "Deployment: Started",
            "ResourceType": "Application"
        }
    ]
}
```

Pour ajouter une balise à une règle de notification (AWS CLI)

1. À partir d'un terminal ou d'une invite de commande, exécutez la commande tag-resource. Par exemple, utilisez la commande suivante pour ajouter une paire clé-valeur de balise portant le nom *Team* et ayant la valeur *Li_Juan*.

```
aws codestar-notifications tag-resource --arn arn:aws:codestar-notifications:us-
east-1:123456789012:notificationrule/fe1efd35-EXAMPLE --tags Team=Li_Juan
```

2. Le résultat produit lors de l'exécution de cette commande est semblable à ce qui suit :

```
{
    "Tags": {
        "Team": "Li_Juan"
    }
}
```

Affichage des règles de notification

Vous pouvez utiliser la console Outils pour développeurs ou la AWS CLI pour afficher toutes les règles de notification pour toutes les ressources d'une région AWS. Vous pouvez également afficher les détails de chaque règle de notification. Contrairement au processus de création d'une règle de notification, vous n'avez pas besoin d'accéder à la page des ressources correspondante.

Pour afficher les règles de notification (console)

1. Ouvrez la console Outils pour développeurs AWS à l'adresse https://console.aws.amazon.com/codesuite/settings/notifications.
2. Dans la barre de navigation, développez Settings (Paramètres), puis choisissez Notification rules (Règles de notification).
3. Dans Notification rules (Règles de notification), passez en revue la liste des règles configurées pour les ressources de votre compte Compte AWS dans la région Région AWS où vous êtes actuellement connecté. Utilisez le sélecteur pour modifier la Région AWS.
4. Pour afficher les détails d'une règle de notification spécifique, choisissez-la dans la liste, puis choisissez View details (Afficher les détails). Vous pouvez également simplement choisir son nom dans la liste.

Pour afficher une liste de règles de notification (AWS CLI)

1. À partir d'un terminal ou d'une invite de commande, exécutez la commande list-notification-rules pour afficher la liste de toutes les règles de notification pour la région AWS spécifiée.

```
aws codestar-notifications list-notification-rules --region us-east-1
```

2. En cas de réussite, cette commande renvoie l'ID et l'ARN de chaque règle de notification de la région AWS, comme suit :

```
{
    "NotificationRules": [
        {
            "Id": "dc82df7a-EXAMPLE",
            "Arn": "arn:aws:codestar-notifications:us-
east-1:123456789012:notificationrule/dc82df7a-EXAMPLE"
        },
        {
            "Id": "8d1f0983-EXAMPLE",
            "Arn": "arn:aws:codestar-notifications:us-
east-1:123456789012:notificationrule/8d1f0983-EXAMPLE"
        }
    ]
}
```

Pour afficher les détails d'une règle de notification (AWS CLI)

1. À partir d'un terminal ou d'une invite de commande, exécutez la commande describe-notification-rule, en spécifiant l'ARN de la règle de notification.

```
aws codestar-notifications describe-notification-rule --arn arn:aws:codestar-
notifications:us-east-1:123456789012:notificationrule/dc82df7a-EXAMPLE
```

2. Si elle aboutit, la commande renvoie un résultat semblable au suivant :

```
{
    "LastModifiedTimestamp": 1569199844.857,
    "EventTypes": [
        {
            "ServiceName": "CodeCommit",
            "EventTypeName": "Branches and tags: Created",
            "ResourceType": "Repository",
            "EventTypeId": "codecommit-repository-branches-and-tags-created"
        }
    ],
```

```
    "Status": "ENABLED",
    "DetailType": "FULL",
    "Resource": "arn:aws:codecommit:us-east-1:123456789012:MyDemoRepo",
    "Arn": "arn:aws:codestar-notifications:us-east-1:123456789012:notificationrule/
dc82df7a-EXAMPLE",
    "Targets": [
        {
            "TargetStatus": "ACTIVE",
            "TargetAddress": "arn:aws:sns:us-
east-1:123456789012:MyNotificationTopic",
            "TargetType": "SNS"
        }
    ],
    "Name": "MyNotificationRule",
    "CreatedTimestamp": 1569199844.857,
    "CreatedBy": "arn:aws:iam::123456789012:user/Mary_Major"
}
```

Pour afficher une liste de balises pour une règle de notification (AWS CLI)

1. À partir d'un terminal ou d'une invite de commande, exécutez la commande list-tags-for-resource pour afficher toutes les balises pour un ARN de règle de notification spécifié.

```
aws codestar-notifications list-tags-for-resource --arn arn:aws:codestar-
notifications:us-east-1:123456789012:notificationrule/fe1efd35-EXAMPLE
```

2. Si elle aboutit, cette commande renvoie un résultat similaire à ce qui suit.

```
{
    "Tags": {
        "Team": "Li_Juan"
    }
}
```

Modification d'une règle de notification

Vous pouvez modifier une règle de notification existante pour modifier son nom, les événements pour lesquels elle envoie des notifications ou les cibles auxquelles elle envoie des notifications. Vous pouvez utiliser la console Outils pour développeurs ou la AWS CLI pour modifier une règle de notification.

Pour modifier une règle de notification (console)

1. Ouvrez la console Outils pour développeurs AWS à l'adresse https://console.aws.amazon.com/codesuite/settings/notifications.
2. Dans la barre de navigation, développez Settings (Paramètres), puis choisissez Notification rules (Règles de notification).
3. Dans Notification rules (Règles de notification), passez en revue la liste des règles configurées pour les ressources de votre compte AWS dans la région Région AWS où vous êtes actuellement connecté. Utilisez le sélecteur pour modifier la Région AWS.
4. Choisissez la règle dans la liste, puis choisissez Edit (Modifier). Effectuez les modifications, puis choisissez Submit (Envoyer).

Pour modifier une règle de notification (AWS CLI)

1. À partir d'un terminal ou d'une invite de commande, exécutez la commande describe-notification-rule pour afficher la structure de la règle de notification.
2. Exécutez la commande update-notification rule pour générer le squelette JSON et enregistrez-le dans un fichier.

```
aws codestar-notifications update-notification-rule --generate-cli-skeleton
 > update.json
```

Vous pouvez donner au fichier le nom de votre choix. Dans cet exemple, le fichier est *update.json*.

3. Ouvrez le fichier JSON dans un éditeur de texte brut et apportez des modifications à la règle.

L'exemple suivant montre une règle de notification nommée **MyNotificationRule** pour un référentiel nommé *MyDemoRepo* dans un compte AWS avec l'ID *123456789012*. Les notifications sont envoyées à une rubrique Amazon SNS nommée *myNotificationTopic* lorsque les branches et les balises sont créées. Le nom de la règle est remplacé par *MyNewNotificationRule* :

```
{
    "Name": "MyNewNotificationRule",
    "EventTypeIds": [
        "codecommit-repository-branches-and-tags-created"
    ],
```

```
    "Resource": "arn:aws:codecommit:us-east-1:123456789012:MyDemoRepo",
    "Targets": [
        {
            "TargetType": "SNS",
            "TargetAddress": "arn:aws:sns:us-
east-1:123456789012:MyNotificationTopic"
        }
    ],
    "Status": "ENABLED",
    "DetailType": "FULL"
}
```

Sauvegardez le fichier.

4. À l'aide du fichier que vous venez de modifier, à partir du terminal ou de la ligne de commande, exécutez à nouveau la commande update-notification-rule pour mettre à jour la règle de notification.

```
aws codestar-notifications update-notification-rule --cli-input-json
 file://update.json
```

5. En cas de réussite, la commande renvoie l'Amazon Resource Name (ARN) de la règle de notification, comme suit :

```
{
    "Arn": "arn:aws:codestar-notifications:us-east-1:123456789012:notificationrule/
dc82df7a-EXAMPLE"
}
```

Pour supprimer une balise d'une règle de notification (AWS CLI)

1. À partir d'un terminal ou d'une invite de commande, exécutez la commande untag-resource. Par exemple, la commande suivante supprime une balise portant le nom de *Team*.

```
aws codestar-notifications untag-resource --arn arn:aws:codestar-notifications:us-
east-1:123456789012:notificationrule/fe1efd35-EXAMPLE --tag-keys Team
```

2. Si elle aboutit, cette commande ne renvoie rien.

Consulter aussi

- Ajouter ou supprimer une cible pour une règle de notification
- Activation ou désactivation des notifications pour une règle de notification
- Événements

Activation ou désactivation des notifications pour une règle de notification

Lorsque vous créez une règle de notification, les notifications sont activées par défaut. Vous n'avez pas à supprimer la règle pour l'empêcher d'envoyer des notifications. Vous pouvez simplement modifier son état de notification.

Pour modifier le statut de notification d'une règle de notification (console)

1. Ouvrez la console Outils pour développeurs AWS à l'adresse https://console.aws.amazon.com/codesuite/settings/notifications.
2. Dans la barre de navigation, développez Settings (Paramètres), puis choisissez Notification rules (Règles de notification).
3. Dans Notification rules (Règles de notification), passez en revue la liste des règles configurées pour les ressources de votre compte AWS dans la région Région AWS où vous êtes actuellement connecté. Utilisez le sélecteur pour modifier la Région AWS.
4. Recherchez la règle de notification que vous souhaitez activer ou désactiver, puis sélectionnez-la pour afficher ses détails.
5. Dans Statut de notification, choisissez le curseur pour modifier le statut de la règle :
   - Sending notifications (Envoi de notifications): il s'agit de la valeur par défaut.
   - Notifications en pause : aucune notification n'est envoyée aux cibles spécifiées.

Pour modifier le statut de notification d'une règle de notification (AWS CLI)

1. Suivez les étapes décrites dans Pour modifier une règle de notification (AWS CLI) pour obtenir le JSON pour la règle de notification.
2. Modifiez le champ `Status` en `ENABLED` (par défaut) ou `DISABLED` (aucune notification), puis exécutez la commande update-notification-rule pour modifier l'état.

```
"Status": "ENABLED"
```

Suppression d'une règle de notification

Il ne peut y avoir que 10 règles de notification configurées pour une ressource. Pensez donc à supprimer les règles dont vous n'avez plus besoin. Vous pouvez utiliser la console Outils pour développeurs ou la AWS CLI pour supprimer une règle de notification.

> **Note**
>
> Vous ne pouvez pas annuler la suppression d'une règle de notification, mais vous pouvez la recréer. La suppression d'une règle de notification ne supprime pas la cible.

Pour supprimer une règle de notification (console)

1. Ouvrez la console Outils pour développeurs AWS à l'adresse https://console.aws.amazon.com/codesuite/settings/notifications.
2. Dans la barre de navigation, développez Settings (Paramètres), puis choisissez Notification rules (Règles de notification).
3. Dans Notification rules (Règles de notification), passez en revue la liste des règles configurées pour les ressources de votre compte AWS dans la région Région AWS où vous êtes actuellement connecté. Utilisez le sélecteur pour modifier la Région AWS.
4. Choisissez la règle de notification, puis choisissez Delete (Supprimer).
5. Saisissez **`delete`**, puis sélectionnez Delete (Supprimer).

Pour supprimer une règle de notification (AWS CLI)

1. À partir d'un terminal ou d'une invite de commande, exécutez la commande delete-notification-rule, en spécifiant l'ARN de la règle de notification.

```
aws codestar-notifications delete-notification-rule --arn arn:aws:codestar-notifications:us-east-1:123456789012:notificationrule/dc82df7a-EXAMPLE
```

2. En cas de réussite, la commande renvoie l'ARN de la règle de notification supprimée, comme suit :

```
{
    "Arn": "arn:aws:codestar-notifications:us-east-1:123456789012:notificationrule/dc82df7a-EXAMPLE"
```

```
}
```

Utilisation des cibles de règle de notification

Une cible de règle de notification est une destination qui définit l'endroit où vous souhaitez que les notifications soient envoyées lorsque les conditions d'événement d'une règle de notification sont satisfaites. Vous pouvez choisir entre les rubriques Amazon SNS et les clients AWS Chatbot configurés pour les canaux Slack ou Microsoft Teams. Vous pouvez créer une rubrique Amazon SNS en tant que cible dans le cadre de la création d'une règle de notification (recommandé). Vous pouvez également choisir une rubrique Amazon SNS existante dans la même région AWS que la règle de notification, mais vous devez la configurer avec la stratégie requise. Si vous choisissez d'utiliser un client AWS Chatbot comme cible, vous devez d'abord créer ce client dans AWS Chatbot.

Si vous souhaitez étendre la portée des notifications, vous pouvez configurer manuellement l'intégration entre les notifications et AWS Chatbot afin que les notifications soient envoyées aux salles de discussion Amazon Chime. Vous pouvez ensuite choisir la rubrique Amazon SNS configurée pour ce client AWS Chatbot comme cible de la règle de notification. Pour de plus amples informations, veuillez consulter Pour intégrer les notifications avec AWS Chatbot et Amazon Chime.

Vous pouvez utiliser la console Outils pour développeurs ou la AWS CLI pour gérer des cibles de notification. Vous pouvez utiliser la console ou la AWS CLI pour créer et configurer des rubriques Amazon SNS et des clients AWS Chatbot en tant que cibles. Vous pouvez également configurer l'intégration entre les rubriques Amazon SNS que vous configurez en tant que cibles et AWS Chatbot. Cela vous permet d'envoyer des notifications aux salles de discussion Amazon Chime. Pour de plus amples informations, veuillez consulter Configurer l'intégration entre les notifications et AWS Chatbot.

Rubriques

- Création ou configuration d'une cible de règle de notification
- Affichage des cibles de règle de notification
- Ajouter ou supprimer une cible pour une règle de notification
- Suppression d'une cible de règle de notification

Création ou configuration d'une cible de règle de notification

Les cibles de règle de notification sont des rubriques Amazon SNS ou des clients AWS Chatbot configurés pour les canaux Slack ou Microsoft Teams.

Un client AWS Chatbot doit être créé pour que vous puissiez sélectionner un client comme cible. Lorsque vous choisissez un client AWS Chatbot comme cible pour une règle de notification, une rubrique Amazon SNS est configurée pour ce client AWS Chatbot avec toutes les stratégies requises pour que les notifications soient envoyées au canal Slack ou Microsoft Teams. Vous n'avez pas à configurer les rubriques Amazon SNS existantes pour le client AWS Chatbot.

Vous pouvez créer des cibles de règle de notification Amazon SNS dans la console Outils pour développeurs lorsque vous créez une règle de notification. La stratégie qui permet d'envoyer des notifications à cette rubrique est appliquée automatiquement. C'est le moyen le plus simple de créer une cible pour une règle de notification. Pour de plus amples informations, veuillez consulter Création d'une règle de notification.

Si vous utilisez une rubrique Amazon SNS existante, vous devez la configurer avec une stratégie d'accès qui permet à la ressource d'envoyer des notifications à cette rubrique. Pour voir un exemple, consultez Configurer une rubrique Amazon SNS pour les notifications.

> **Note**
>
> Si vous souhaitez utiliser une rubrique Amazon SNS existante au lieu d'en créer une nouvelle, dans Targets (Cibles), choisissez son ARN. Assurez-vous que la rubrique dispose de la stratégie d'accès appropriée et que la liste d'abonnés contient uniquement les utilisateurs autorisés à voir des informations sur le pipeline. Si la rubrique Amazon SNS est une rubrique qui a été utilisée pour les notifications CodeCommit avant le 5 novembre 2019, elle contient une stratégie qui permet à CodeCommit publier sur cette rubrique et qui contient des autorisations différentes de celles requises pour AWS CodeStar Notifications. L'utilisation de ces rubriques n'est pas recommandée. Si vous souhaitez utiliser une rubrique créée pour cette expérience, vous devez ajouter la stratégie requise pour AWS CodeStar Notifications en plus de celle qui existe déjà. Pour plus d'informations, consultez Configurer une rubrique Amazon SNS pour les notifications et Présentation du contenu des notifications et de la sécurité.

Si vous souhaitez étendre la portée des notifications, vous pouvez configurer manuellement l'intégration entre les notifications et AWS Chatbot afin que les notifications soient envoyées aux salles de discussion Amazon Chime. Pour plus d'informations, consultez Cibles et Pour intégrer les notifications avec AWS Chatbot et Amazon Chime.

Pour configurer une rubrique Amazon SNS existante à utiliser comme cible de règle de notification (console)

1. Connectez-vous à AWS Management Console et ouvrez la console Amazon SNS à l'adresse https://console.aws.amazon.com/sns/v3/home.
2. Dans la barre de navigation, sélectionnez Topics (Rubriques). Choisissez la rubrique, puis choisissez Edit (Modifier).
3. Développer Access policy (Stratégie d'accès), puis choisissez Advanced (Avancé).
4. Dans l'éditeur JSON, ajoutez la déclaration suivante à la stratégie. Inclure l'ARN de la rubrique, Région AWS, l'ID Compte AWS et le nom de la rubrique.

```
 {
      "Sid": "AWSCodeStarNotifications_publish",
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "codestar-notifications.amazonaws.com"
        ]
      },
      "Action": "SNS:Publish",
      "Resource": "arn:aws:sns:us-east-2:123456789012:codestar-notifications-
MyTopicForNotificationRules"
    }
```

Cette déclaration de stratégie doit ressembler à l'exemple suivant.

```
{
  "Version": "2008-10-17",
  "Id": "__default_policy_ID",
  "Statement": [
    {
      "Sid": "__default_statement_ID",
      "Effect": "Allow",
      "Principal": {
        "AWS": "*"
      },
      "Action": [
        "SNS:GetTopicAttributes",
        "SNS:SetTopicAttributes",
        "SNS:AddPermission",
        "SNS:RemovePermission",
```

```
        "SNS:DeleteTopic",
        "SNS:Subscribe",
        "SNS:ListSubscriptionsByTopic",
        "SNS:Publish",
        "SNS:Receive"
      ],
      "Resource": "arn:aws:sns:us-east-2:123456789012:codestar-notifications-
MyTopicForNotificationRules",
      "Condition": {
        "StringEquals": {
          "AWS:SourceOwner": "123456789012"
        }
      }
    },
 {
      "Sid": "AWSCodeStarNotifications_publish",
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "codestar-notifications.amazonaws.com"
        ]
      },
      "Action": "SNS:Publish",
      "Resource": "arn:aws:sns:us-east-2:123456789012:codestar-notifications-
MyTopicForNotificationRules"
    }
  ]
}
```

5. Sélectionnez Save Changes (Enregistrer les modifications).
6. Dans Subscriptions (Abonnements), consultez la liste des abonnés à la rubrique. Ajoutez, modifiez ou supprimez des abonnés en fonction des besoins pour cette cible de règle de notification. Assurez-vous que la liste d'abonnés contient uniquement les utilisateurs autorisés à afficher des informations sur la ressource. Pour de plus amples informations, veuillez consulter Présentation du contenu des notifications et de la sécurité.

Pour créer un client AWS Chatbot avec Slack à utiliser comme cible

1. Suivez les instructions de Configuration d'AWS Chatbot avec Slack dans le Guide de l'administrateur AWS Chatbot. Dans cette situation, vous devez envisager les options suivantes pour une intégration optimale avec les notifications :

- Lors de la création d'un rôle IAM, vous pouvez choisir un nom de rôle qui facilite l'identification de l'objet de ce rôle (par exemple, **`AWSCodeStarNotifications-Chatbot-Slack-Role`**). Cela peut vous aider à identifier l'objet du rôle à l'avenir.
- Dans les rubriques SNS, vous n'avez pas à choisir une rubrique ou une région AWS. Lorsque vous choisissez le client AWS Chatbot comme cible, une rubrique Amazon SNS avec toutes les autorisations requises est créée et configurée pour le client AWS Chatbot dans le cadre du processus de création de règle de notification.

2. Terminez le processus de création du client. Vous pouvez alors choisir ce client comme cible lors de la création de règles de notification. Pour de plus amples informations, veuillez consulter Création d'une règle de notification.

> **Note**
>
> Ne supprimez pas la rubrique Amazon SNS du client AWS Chatbot une fois qu'elle a été configurée pour vous. Cela empêchera l'envoi de notifications à Slack.

Pour créer un client AWS Chatbot avec Microsoft Teams à utiliser comme cible

1. Suivez les instructions de Configuration de AWS Chatbot avec Microsoft Teams dans le Guide de l'administrateur AWS Chatbot. Dans cette situation, vous devez envisager les options suivantes pour une intégration optimale avec les notifications :

   - Lors de la création d'un rôle IAM, vous pouvez choisir un nom de rôle qui facilite l'identification de l'objet de ce rôle (par exemple, **`AWSCodeStarNotifications-Chatbot-Microsoft-Teams-Role`**). Cela peut vous aider à identifier l'objet du rôle à l'avenir.
   - Dans les rubriques SNS, vous n'avez pas à choisir une rubrique ou une région AWS. Lorsque vous choisissez le client AWS Chatbot comme cible, une rubrique Amazon SNS avec toutes les autorisations requises est créée et configurée pour le client AWS Chatbot dans le cadre du processus de création de règle de notification.

2. Terminez le processus de création du client. Vous pouvez alors choisir ce client comme cible lors de la création de règles de notification. Pour de plus amples informations, veuillez consulter Création d'une règle de notification.

> **Note**
>
> Ne supprimez pas la rubrique Amazon SNS du client AWS Chatbot une fois qu'elle a été configurée pour vous. Cela empêchera l'envoi de notifications à Microsoft Teams.

Affichage des cibles de règle de notification

Vous pouvez utiliser Outils pour développeurs, et non la console Amazon SNS pour afficher toutes les cibles de règle de notification pour toutes les ressources d'une région AWS. Vous pouvez également afficher les détails d'une cible de règle de notification spécifique.

Pour afficher les cibles de règle de notification (console)

1. Ouvrez la console Outils pour développeurs AWS à l'adresse https://console.aws.amazon.com/codesuite/settings/notifications.
2. Dans la barre de navigation, développez Settings (Paramètres), puis choisissez Notification rules (Règles de notification).
3. Dans Notification rule targets (Cibles de règle de notification), passez en revue la liste des cibles utilisées par les règles de notification de votre Compte AWS dans la Région AWS où vous êtes actuellement connecté. Utilisez le sélecteur pour modifier la Région AWS. Si l'état de la cible est Inaccessible, vous pouvez avoir besoin d'effectuer une enquête. Pour de plus amples informations, veuillez consulter Résolution des problèmes .

Pour afficher la liste des cibles de règle de notification (AWS CLI)

1. À partir d'un terminal ou d'une invite de commande, exécutez la commande list-targets pour afficher la liste de toutes les cibles de règle de notification pour la région AWS spécifiée :

```
aws codestar-notifications list-targets --region us-east-2
```

2. En cas de réussite, cette commande renvoie l'ID et l'ARN de chaque règle de notification de la région AWS, comme suit :

```
{
    "Targets": [
        {
```

```
            "TargetAddress": "arn:aws:sns:us-
east-2:123456789012:MySNSTopicForNotificationRules",
            "TargetType": "SNS",
            "TargetStatus": "ACTIVE"
        },
        {
            "TargetAddress": "arn:aws:chatbot::123456789012:chat-configuration/
slack-channel/MySlackChannelClientForMyDevTeam",
            "TargetStatus": "ACTIVE",
            "TargetType": "AWSChatbotSlack"
        },
        {
            "TargetAddress": "arn:aws:sns:us-
east-2:123456789012:MySNSTopicForNotificationsAboutMyDemoRepo",
            "TargetType": "SNS",
            "TargetStatus": "ACTIVE"
        }
    ]
}
```

Ajouter ou supprimer une cible pour une règle de notification

Vous pouvez modifier une règle de notification existante pour modifier la ou les cibles auxquelles elle envoie des notifications. Vous pouvez utiliser la console Outils pour développeurs ou la AWS CLI pour modifier des cibles de règle de notification.

Pour modifier les cibles d'une règle de notification (console)

1. Ouvrez la console Outils pour développeurs AWS à l'adresse https://console.aws.amazon.com/codesuite/settings/notifications.
2. Dans la barre de navigation, développez Settings (Paramètres), puis choisissez Notification rules (Règles de notification).
3. Dans Notification rules (Règles de notification), passez en revue la liste des règles configurées pour les ressources de votre compte AWS dans la Région AWS où vous êtes actuellement connecté. Utilisez le sélecteur pour modifier la Région AWS.
4. Choisissez la règle, puis choisissez Edit (Modifier).
5. Dans Targets (Cibles), effectuez l'une des actions suivantes :

- Pour ajouter une cible supplémentaire, choisissez Ajouter une cible, puis choisissez la rubrique Amazon SNS ou le client AWS Chatbot (Slack) ou AWS Chatbot (Microsoft Teams) que vous souhaitez ajouter à partir de la liste. Vous pouvez également choisir Créer une rubrique SNS pour créer une rubrique et l'ajouter en tant que cible. Une règle de notification peut comporter jusqu'à 10 cibles.
- Pour supprimer une cible, choisissez Remove target (Supprimer la cible) en regard de la cible que vous souhaitez supprimer.

6. Sélectionnez Submit (Envoyer).

Pour ajouter une cible à une règle de notification (AWS CLI)

1. À partir d'un terminal ou d'une invite de commandes, exécutez la commande subscribe pour ajouter une cible. Par exemple, la commande suivante ajoute une rubrique Amazon SNS en tant que cible pour une règle de notification.

```
aws codestar-notifications subscribe --arn arn:aws:codestar-
notifications:us-east-1:123456789012:notificationrule/dc82df7a-
EXAMPLE --target TargetType=SNS,TargetAddress=arn:aws:sns:us-
east-1:123456789012:MyNotificationTopic
```

2. En cas de réussite, la commande renvoie l'ARN de la règle de notification mise à jour, comme suit :

```
{
    "Arn": "arn:aws:codestar-notifications:us-east-1:123456789012:notificationrule/
dc82df7a-EXAMPLE"
}
```

Pour supprimer une cible d'une règle de notification (AWS CLI)

1. À partir d'un terminal ou d'une invite de commandes, exécutez la commande unsubscribe pour supprimer une cible. Par exemple, la commande suivante supprime une rubrique Amazon SNS en tant que cible pour une règle de notification.

```
aws codestar-notifications unsubscribe --arn arn:aws:codestar-
notifications:us-east-1:123456789012:notificationrule/dc82df7a-
```

```
EXAMPLE --target TargetType=SNS,TargetAddress=arn:aws:sns:us-
east-1:123456789012:MyNotificationTopic
```

2. En cas de réussite, la commande renvoie l'ARN de la règle de notification mise à jour et les informations sur la cible supprimée, comme suit :

```
{
    "Arn": "arn:aws:codestar-notifications:us-east-1:123456789012:notificationrule/
dc82df7a-EXAMPLE"
    "TargetAddress": "arn:aws:sns:us-east-1:123456789012:MyNotificationTopic"
}
```

Consulter aussi

- Modification d'une règle de notification
- Activation ou désactivation des notifications pour une règle de notification

Suppression d'une cible de règle de notification

Vous pouvez supprimer une cible si elle n'est plus nécessaire. Seules 10 cibles de règle de notification peuvent être configurées pour une ressource. Par conséquent, la suppression des cibles inutiles peut permettre de créer de la place pour les autres cibles que vous pourriez souhaiter ajouter à cette règle de notification.

> **Note**
>
> La suppression d'une cible de règle de notification supprime la cible de toutes les règles de notification configurées pour l'utiliser comme cible, mais elle ne supprime pas la cible elle-même.

Pour supprimer une cible de règle de notification (console)

1. Ouvrez la console Outils pour développeurs AWS à l'adresse https://console.aws.amazon.com/codesuite/settings/notifications.
2. Dans la barre de navigation, développez Settings (Paramètres), puis choisissez Notification rules (Règles de notification).

3. Dans Notification rule targets (Cibles de règle de notification), passez en revue la liste des cibles configurées pour les ressources de votre compte AWS dans la Région AWS où vous êtes actuellement connecté. Utilisez le sélecteur pour modifier la Région AWS.
4. Choisissez la cible de la règle de notification, puis choisissez Delete (Supprimer).
5. Saisissez **`delete`**, puis sélectionnez Delete (Supprimer).

Pour supprimer une cible de règle de notification (AWS CLI)

1. À partir d'un terminal ou d'une invite de commande, exécutez la commande delete-target, en spécifiant l'ARN de la cible. Par exemple, la commande suivante supprime une cible qui utilise une rubrique Amazon SNS.

```
aws codestar-notifications delete-target --target-address arn:aws:sns:us-
east-1:123456789012:MyNotificationTopic
```

2. En cas de réussite, la commande ne renvoie rien. En cas d'échec, la commande renvoie une erreur. L'erreur la plus courante est que la rubrique soit la cible d'une ou plusieurs règles de notification.

```
An error occurred (ValidationException) when calling the DeleteTarget operation:
 Unsubscribe target before deleting.
```

Vous pouvez utiliser le paramètre `--force-unsubscribe-all` pour supprimer automatiquement la cible de toutes les règles de notification configurées pour l'utiliser comme cible, puis supprimer la cible elle-même.

```
aws codestar-notifications delete-target --target-address arn:aws:sns:us-
east-1:123456789012:MyNotificationTopic --force-unsubscribe-all
```

Configurer l'intégration entre les notifications et AWS Chatbot

AWS Chatbot est un service AWS qui permet aux équipes DevOps et de développement logiciel d'utiliser les salles de conversation Amazon Chime, les canaux Slack et les canaux Microsoft Teams pour surveiller les événements opérationnels et y répondre dans le AWS Cloud. Vous pouvez configurer l'intégration entre les cibles de règle de notification et AWS Chatbot afin que les notifications sur les événements s'affichent dans l'espace de conversation Amazon Chime, le

canal Slack ou le canal Microsoft Teams que vous choisissez. Pour en savoir plus, consultez la documentation AWS Chatbot.

Avant de configurer l'intégration à AWS Chatbot, vous devez configurer une règle de notification et une cible de règle. Pour plus d'informations, consultez Configuration et Création d'une règle de notification. Vous devez également configurer un canal Slack, un canal Microsoft Teams ou une salle de conversation Amazon Chime dans AWS Chatbot. Pour plus d'informations, consultez la documentation de ces services.

Rubriques

- Configurer un client AWS Chatbot pour un canal Slack
- Configurer un client AWS Chatbot pour un canal Microsoft Teams
- Configurer manuellement les clients pour Slack ou Amazon Chime

Configurer un client AWS Chatbot pour un canal Slack

Vous pouvez créer des règles de notification qui utilisent un client AWS Chatbot comme cible. Si vous créez un client pour un canal Slack, vous pouvez l'utiliser directement comme cible dans le flux de travail pour créer une règle de notification. C'est le moyen le plus simple de configurer les notifications qui apparaissent dans les canaux Slack.

Pour créer un client AWS Chatbot avec Slack à utiliser comme cible

1. Suivez les instructions de Configuration d'AWS Chatbot avec Slack dans le Guide de l'administrateur AWS Chatbot. Dans cette situation, vous devez envisager les options suivantes pour une intégration optimale avec les notifications :

   - Lors de la création d'un rôle IAM, vous pouvez choisir un nom de rôle qui facilite l'identification de l'objet de ce rôle (par exemple, **`AWSCodeStarNotifications-Chatbot-Slack-Role`**). Cela peut vous aider à identifier l'objet du rôle à l'avenir.
   - Dans les rubriques SNS, vous n'avez pas à choisir une rubrique ou une région AWS. Lorsque vous choisissez le client AWS Chatbot comme cible, une rubrique Amazon SNS avec toutes les autorisations requises est créée et configurée pour le client AWS Chatbot dans le cadre du processus de création de règle de notification.

2. Terminez le processus de création du client. Vous pouvez alors choisir ce client comme cible lors de la création de règles de notification. Pour de plus amples informations, veuillez consulter Création d'une règle de notification.

> **Note**
>
> Ne supprimez pas la rubrique Amazon SNS du client AWS Chatbot une fois qu'elle a été configurée pour vous. Cela empêchera l'envoi de notifications à Slack.

Configurer un client AWS Chatbot pour un canal Microsoft Teams

Vous pouvez créer des règles de notification qui utilisent un client AWS Chatbot comme cible. Si vous créez un client pour un canal Microsoft Teams, vous pouvez l'utiliser directement comme cible dans le flux de travail pour créer une règle de notification. C'est le moyen le plus simple de configurer les notifications qui apparaissent dans les canaux Microsoft Teams.

Pour créer un client AWS Chatbot avec Microsoft Teams à utiliser comme cible

1. Suivez les instructions de Configuration de AWS Chatbot avec Microsoft Teams dans le Guide de l'administrateur AWS Chatbot. Dans cette situation, vous devez envisager les options suivantes pour une intégration optimale avec les notifications :

   - Lors de la création d'un rôle IAM, vous pouvez choisir un nom de rôle qui facilite l'identification de l'objet de ce rôle (par exemple, **`AWSCodeStarNotifications-Chatbot-Microsoft-Teams-Role`**). Cela peut vous aider à identifier l'objet du rôle à l'avenir.
   - Dans les rubriques SNS, vous n'avez pas à choisir une rubrique ou une région AWS. Lorsque vous choisissez le client AWS Chatbot comme cible, une rubrique Amazon SNS avec toutes les autorisations requises est créée et configurée pour le client AWS Chatbot dans le cadre du processus de création de règle de notification.
2. Terminez le processus de création du client. Vous pouvez alors choisir ce client comme cible lors de la création de règles de notification. Pour de plus amples informations, veuillez consulter Création d'une règle de notification.

> **Note**
>
> Ne supprimez pas la rubrique Amazon SNS du client AWS Chatbot une fois qu'elle a été configurée pour vous. Cela empêchera l'envoi de notifications à Microsoft Teams.

Configurer manuellement les clients pour Slack ou Amazon Chime

Vous pouvez choisir de créer l'intégration entre les notifications et Slack ou Amazon Chime directement. Il s'agit de la seule méthode disponible pour configurer les notifications aux salles de discussion Amazon Chime. Lorsque vous configurez cette intégration manuellement, vous créez un client AWS Chatbot qui utilise une rubrique Amazon SNS que vous avez précédemment configurée comme cible pour une règle de notification.

Pour intégrer manuellement les notifications avec AWS Chatbot et Slack

1. Ouvrez la console Outils pour développeurs AWS à l'adresse https://console.aws.amazon.com/codesuite/settings/notifications.
2. Choisissez Settings (Paramètres), puis Notification rules (Règles de notification).
3. Dans Notification rule targets (Cibles de règle de notification), recherchez et copiez la cible.

   > **Note**
   >
   > Vous pouvez configurer plusieurs règles de notification pour utiliser la même rubrique Amazon SNS comme cible. Cela peut vous aider à consolider la messagerie, mais cela peut également avoir des conséquences imprévues si la liste des abonnements est destinée à être spécifique à une règle de notification ou à une ressource.

4. Ouvrez la console AWS Chatbot à l'adresse https://console.aws.amazon.com/chatbot/.
5. Choisissez Configure new client (Configurer un nouveau client), puis Slack.
6. Choisissez Configure (Configurer).
7. Connectez-vous à votre espace de travail Slack.
8. Lorsque vous êtes invité à confirmer les choix, choisissez Allow (Autoriser).
9. Choisissez Configure new client (Configurer un nouveau client).
10. Dans Configuration details (Détails de la configuration), dans Configuration name (Nom de la configuration), entrez un nom pour votre client. Il s'agit du nom qui apparaît dans la liste des cibles disponibles pour le type de cible AWS Chatbot (Slack) lorsque vous créez des règles de notification.
11. Dans Configure Slack Channel (Configurer le canal Slack), pour Channel type (Type de canal), choisissez Public ou Private (Privé), selon le type de canal que vous souhaitez utiliser pour l'intégration.

- Dans Public channel (Canal public), choisissez le nom du canal Slack dans la liste.
- Dans Private channel ID (ID de canal privé), entrez le code de canal ou l'URL.

12. Dans IAM permissions (Autorisations IAM), dans Role (Rôle), choisissez Create an IAM role using a template (Créer un rôle IAM à l'aide d'un modèle). Dans Policy templates (Modèles de stratégie), choisissez Notification permissions (Autorisations de notification). Dans Role name (Nom du rôle), saisissez le nom de ce rôle, par exemple **`AWSCodeStarNotifications-Chatbot-Slack-Role`**. Dans Policy templates (Modèles de stratégie), choisissez Notification permissions (Autorisations de notification).
13. Dans SNS topics (Rubriques SNS), pour SNS Region (Région SNS), choisissez la Région AWS dans laquelle vous avez créé la cible de règle de notification. Dans SNS topics (Rubriques SNS), choisissez le nom de la rubrique Amazon SNS que vous avez configurée comme cible de règle de notification.

> **Note**
>
> Cette étape n'est pas nécessaire si vous créez une règle de notification utilisant ce client comme cible.

14. Choisissez Configure (Configurer).

> **Note**
>
> Si vous avez configuré l'intégration avec un canal privé, vous devez inviter AWS Chatbot sur le canal avant de voir les notifications sur ce canal. Pour en savoir plus, consultez la documentation AWS Chatbot.

15. (Facultatif) Afin de tester l'intégration, modifiez la ressource qui correspond à un type d'événement pour une règle de notification qui est configurée pour utiliser la rubrique Amazon SNS comme cible. Par exemple, si vous avez une règle de notification configurée pour envoyer des notifications lorsque des commentaires sont effectués sur une demande d'extraction, faites un commentaire sur une demande d'extraction, puis regardez le canal Slack dans le navigateur pour voir quand la notification s'affiche.

Pour intégrer les notifications avec AWS Chatbot et Amazon Chime

1. Ouvrez la console Outils pour développeurs AWS à l'adresse https://console.aws.amazon.com/codesuite/settings/notifications.
2. Choisissez Settings (Paramètres), puis Notification rules (Règles de notification).
3. Dans Notification rule targets (Cibles de règle de notification), recherchez et copiez la cible.

   > **Note**
   >
   > Vous pouvez configurer plusieurs règles de notification pour utiliser la même rubrique Amazon SNS comme cible. Cela peut vous aider à consolider la messagerie, mais cela peut également avoir des conséquences imprévues si la liste des abonnements est destinée à être spécifique à une règle de notification ou à une ressource.

4. Dans Amazon Chime, ouvrez la salle de conversation que vous souhaitez configurer pour l'intégration.
5. Choisissez l'icône d'engrenage dans le coin supérieur droit, puis choisissez Manage webhooks (Gérer les webhooks).
6. Dans la boîte de dialogue Manage webhooks (Gérer les webhooks), choisissez New (Nouveau), saisissez un nom pour le webhook et choisissez Create (Créer).
7. Vérifiez que le webhook apparaît, puis choisissez Copy webhook URL (Copier l'URL du webhook).
8. Ouvrez la console AWS Chatbot à l'adresse https://console.aws.amazon.com/chatbot/.
9. Choisissez Configure new client (Configurer un nouveau client), puis choisissez Amazon Chime.
10. Dans Configuration details (Détails de la configuration), dans Configuration name (Nom de la configuration), entrez un nom pour votre client.
11. Dans Webhook URL (URL du webhook), collez l'URL. Dans la Webhook description (Description du webhook), fournissez une description facultative.
12. Dans IAM permissions (Autorisations IAM), dans Role (Rôle), choisissez Create an IAM role using a template (Créer un rôle IAM à l'aide d'un modèle). Dans Policy templates (Modèles de stratégie), choisissez Notification permissions (Autorisations de notification). Dans Role name (Nom du rôle), saisissez le nom de ce rôle, par exemple **`AWSCodeStarNotifications-Chatbot-Chime-Role`**.
13. Dans SNS topics (Rubriques SNS), pour SNS Region (Région SNS), choisissez la Région AWS dans laquelle vous avez créé la cible de règle de notification. Dans SNS topics (Rubriques SNS),

choisissez le nom de la rubrique Amazon SNS que vous avez configurée comme cible de règle de notification.

14. Choisissez Configure (Configurer).
15. (Facultatif) Afin de tester l'intégration, modifiez la ressource qui correspond à un type d'événement pour une règle de notification qui est configurée pour utiliser la rubrique Amazon SNS comme cible. Par exemple, si vous avez une règle de notification configurée pour envoyer des notifications lorsque des commentaires sont effectués sur une demande d'extraction, faites un commentaire sur une demande d'extraction, puis regardez la salle de conversation Amazon Chime pour voir quand la notification s'affiche dans cette salle.

Journalisation des appels d'API de notification CodeStar AWS avec AWS CloudTrail

AWS CodeStar Notifications est intégré à AWS CloudTrail, un service qui enregistre les actions effectuées par un utilisateur, un rôle ou un service AWS. CloudTrail capture les appels d'API pour les notifications en tant qu'événements. Les appels capturées incluent des appels de la console Outils pour développeurs et le code des appels vers les opérations d'API AWS CodeStar Notifications. Si vous créez un journal d'activité, vous pouvez activer la livraison continue d'événements CloudTrail à un compartiment Amazon S3, y compris des événements pour les notifications. Si vous ne configurez pas de journal d'activité, vous pouvez toujours afficher les événements les plus récents dans la console CloudTrail dans Event history (Historique des événements). Avec les informations collectées par CloudTrail, vous pouvez déterminer la demande qui a été envoyée à AWS CodeStar Notifications, l'adresse IP à partir de laquelle la demande a été effectuée, l'auteur et la date de la demande, ainsi que d'autres détails.

Pour plus d'informations, consultez le AWS CloudTrailGuide de l'utilisateur .

Informations sur AWS CodeStar Notifications dans CloudTrail

CloudTrail est activé dans votre Compte AWS lors de la création de ce dernier. Lorsqu'une activité se produit dans AWS CodeStar Notifications, elle est enregistrée au sein d'un événement CloudTrail avec d'autres événements de services AWS dans Historique des événements. Vous pouvez afficher, rechercher et télécharger les événements récents dans votre Compte AWS. Pour plus d'informations, consultez Affichage des événements avec l'historique des événements CloudTrail.

Pour un enregistrement continu des événements dans votre Compte AWS, notamment des événements concernant AWS CodeStar Notifications, créez un journal de suivi. Un journal d'activité

permet à CloudTrail de distribuer les fichiers journaux vers Simple Storage Service (Amazon S3) bucket. Par défaut, lorsque vous créez un journal d'activité dans la console, il s'applique à toutes les régions Régions AWS. Le journal de suivi consigne les événements de toutes les Régions dans la partition AWS et livre les fichiers journaux dans le compartiment Amazon S3 de votre choix. En outre, vous pouvez configurer d'autres services AWS pour analyser et agir sur les données d'événements collectées dans les journaux CloudTrail. Pour en savoir plus, consultez les ressources suivantes :

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

Toutes les actions AWS CodeStar Notifications sont journalisées par CloudTrail et sont documentées dans la *référence API AWS CodeStar Notifications*. À titre d'exemple, les appels vers les actions `CreateNotificationRule`, `Subscribe` et `ListEventTypes` génèrent des entrées dans les fichiers journaux CloudTrail.

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

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

Pour plus d'informations, consultez l'élément userIdentity CloudTrail.

Présentation des entrées des fichiers journaux

Un journal d'activité est une configuration qui permet d'envoyer les événements dans des fichiers journaux à un compartiment Amazon S3 que vous spécifiez. Les fichiers journaux CloudTrail peuvent contenir une ou plusieurs entrées. Un événement représente une demande unique provenant de n'importe quelle source et comprend des informations sur l'action demandée, la date et l'heure de l'action, les paramètres de la requête, etc. Les fichiers journaux CloudTrail ne constituent pas une série ordonnée retraçant les appels d'API publiques. Ils ne suivent aucun ordre précis.

L'exemple suivant montre une entrée de journal CloudTrail qui illustre la création d'une règle de notification, y compris les actions `CreateNotificationRule` et `Subscribe`.

> **Note**
>
> Certains événements inclus dans les entrées des fichiers journaux peuvent provenir du rôle lié à un service AWSServiceRoleForCodeStarNotifications.


```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type":"IAMUser",
        "principalId":"AIDACKCEVSQ6C2EXAMPLE",
        "arn":"arn:aws:iam::123456789012:user/Mary_Major",
        "accountId":"123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName":"Mary_Major"
    },
    "eventTime": "2019-10-07T21:34:41Z",
    "eventSource": "events.amazonaws.com",
    "eventName": "CreateNotificationRule",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "codestar-notifications.amazonaws.com",
    "userAgent": "codestar-notifications.amazonaws.com",
    "requestParameters": {
        "description": "This rule is used to route CodeBuild, CodeCommit, CodePipeline,
 and other Developer Tools notifications to AWS CodeStar Notifications",
        "name": "awscodestarnotifications-rule",
        "eventPattern": "{\"source\":[\"aws.codebuild\",\"aws.codecommit\",
\"aws.codepipeline\"]}"
    },
    "responseElements": {
        "ruleArn": "arn:aws:events:us-east-1:123456789012:rule/
awscodestarnotifications-rule"
    },
    "requestID": "ff1f309a-EXAMPLE",
    "eventID": "93c82b07-EXAMPLE",
    "eventType": "AwsApiCall",
    "apiVersion": "2015-10-07",
    "recipientAccountId": "123456789012"
}
```

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type":"IAMUser",
        "principalId":"AIDACKCEVSQ6C2EXAMPLE",
        "arn":"arn:aws:iam::123456789012:user/Mary_Major",
        "accountId":"123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName":"Mary_Major"
    },
    "eventTime": "2019-10-07T21:34:41Z",
    "eventSource": "events.amazonaws.com",
    "eventName": "Subscribe",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "codestar-notifications.amazonaws.com",
    "userAgent": "codestar-notifications.amazonaws.com",
    "requestParameters": {
        "targets": [
            {
                "arn": "arn:aws:codestar-notifications:us-east-1:::",
                "id": "codestar-notifications-events-target"
            }
        ],
        "rule": "awscodestarnotifications-rule"
    },
    "responseElements": {
        "failedEntryCount": 0,
        "failedEntries": []
    },
    "requestID": "9466cbda-EXAMPLE",
    "eventID": "2f79fdad-EXAMPLE",
    "eventType": "AwsApiCall",
    "apiVersion": "2015-10-07",
    "recipientAccountId": "123456789012"
}
```

Résolution des problèmes

Les informations suivantes vous aident à résoudre les problèmes courants que vous êtes susceptible de rencontrer avec les notifications.

Rubriques

Je reçois une erreur d'autorisation lorsque j'essaie de créer une règle de notification sur une ressource

Assurez-vous que vous disposez des autorisations suffisantes. Pour de plus amples informations, veuillez consulter Exemples de politiques basées sur l'identité.

Je ne peux pas afficher les règles de notification

Problème : lorsque vous êtes dans la console Outils pour développeurs et que vous choisissez Notifications sous Settings (Paramètres), une erreur d'autorisation s'affiche.

Correctifs possibles : vous ne disposez peut-être pas des autorisations requises pour afficher les notifications. Bien que la plupart des stratégies gérées pour les services AWS Outils pour développeurs, tels que CodeCommit et CodePipeline, incluent des autorisations pour les notifications, les services qui ne prennent pas actuellement en charge les notifications n'incluent pas d'autorisations pour les afficher. Vous pouvez également appliquer une stratégie personnalisée à votre utilisateur ou à votre rôle IAM qui ne vous permet pas d'afficher les notifications. Pour de plus amples informations, veuillez consulter Exemples de politiques basées sur l'identité.

Je ne peux pas créer de règle de notification

Vous ne disposez peut-être pas des autorisations requises pour créer une règle de notification. Pour de plus amples informations, veuillez consulter Exemples de politiques basées sur l'identité.

Je reçois des notifications pour une ressource à laquelle je ne peux pas accéder

Une fois que vous avez créé une règle de notification et ajouté une cible, la fonctionnalité de notifications ne vérifie pas si le destinataire a accès à la ressource. Il est donc possible que vous

receviez des notifications concernant une ressource à laquelle vous ne pouvez pas accéder. Demandez à être supprimé de la liste d'abonnement de la cible si vous ne pouvez pas vous supprimer directement.

Je ne reçois pas les notifications Amazon SNS

Pour résoudre les problèmes liés à la rubrique Amazon SNS, vérifiez les points suivants :

- Assurez-vous que la rubrique Amazon SNS se trouve dans la même région AWS que la règle de notification.
- Vérifiez que votre alias de messagerie est abonné à la bonne rubrique et que vous avez confirmé l'abonnement. Pour plus d'informations, consultez Abonnement d'un point de terminaison à une rubrique Amazon SNS.
- Vérifiez que la stratégie de rubrique a été modifiée pour autoriser AWS CodeStar Notifications à envoyer des notifications push à cette rubrique. La stratégie de rubrique doit inclure une instruction similaire à ce qui suit :

```
{
    "Sid": "AWSCodeStarNotifications_publish",
    "Effect": "Allow",
    "Principal": {
        "Service": [
            "codestar-notifications.amazonaws.com"
        ]
    },
    "Action": "SNS:Publish",
    "Resource": "arn:aws:sns:us-east-1:123456789012:MyNotificationTopicName",
    "Condition": {
        "StringEquals": {
            "aws:SourceAccount": "123456789012"
        }
    }
}
```

  Pour de plus amples informations, veuillez consulter Configurer une rubrique Amazon SNS pour les notifications.

Je reçois des notifications en double à propos d'événements

Voici les raisons les plus courantes pour recevoir plusieurs notifications :

- Plusieurs règles de notification qui incluent le même type d'événement ont été configurées pour une ressource et vous êtes abonné aux rubriques Amazon SNS qui sont les cibles de ces règles. Pour résoudre ce problème, désabonnez-vous de l'une des rubriques ou modifiez les règles de notification pour supprimer la duplication.
- Une ou plusieurs cibles de règle de notification sont intégrées à AWS Chatbot et vous recevez des notifications à la fois dans votre boîte de réception de messagerie et dans un canal Slack, un canal Microsoft Teams ou une salle de conversation Amazon Chime. Pour résoudre ce problème, envisagez de désabonner votre adresse e-mail de la rubrique Amazon SNS qui est la cible de la règle et de consulter les notifications uniquement dans le canal Slack, le canal Microsoft Teams ou la salle de conversation Amazon Chime.

Je veux comprendre pourquoi une cible de notification présente le statut Inaccessible

Les cibles ont deux statuts possibles : Active et Inaccessible. Inaccessible indique que les notifications ont été envoyées à une cible et que leur envoi n'a pas réussi. Les notifications continuent d'être envoyées à cette cible et, si l'envoi réussit, le statut est remplacé par Active.

La cible d'une règle de notification peut devenir indisponible pour l'une des raisons suivantes :

- La ressource (rubrique Amazon SNS ou client AWS Chatbot) a été supprimée. Choisissez une autre cible pour la règle de notification.
- La rubrique Amazon SNS est chiffrée et la stratégie requise pour les rubriques chiffrées est manquante ou la clé AWS KMS a été supprimée. Pour de plus amples informations, veuillez consulter Configurer une rubrique Amazon SNS pour les notifications.
- La rubrique Amazon SNS n'a pas la stratégie requise pour les notifications. Les notifications ne peuvent pas être envoyées à une rubrique Amazon SNS, sauf si elle dispose de la stratégie. Pour de plus amples informations, veuillez consulter Configurer une rubrique Amazon SNS pour les notifications.
- Le service de support de la cible (Amazon SNS ou AWS Chatbot) peut rencontrer des problèmes.

Je souhaite augmenter mes quotas pour les notifications et les ressources

Actuellement, vous ne pouvez pas modifier les quotas. Consultez Quotas pour les notifications.

Quotas pour les notifications

Le tableau suivant répertorie les quotas (également appelés limites) pour les notifications dans la console Outils pour développeurs. Pour plus d'informations sur les limites qui peuvent être modifiées, consultez Quotas de service AWS.

Ressource	Limite par défaut
Nombre maximal de règles de notification dans un compte AWS	1 000
Nombre maximal de cibles pour une règle de notification	10
Nombre maximal de règles de notification pour une ressource	10

Qu'est-ce que les connexions ?

Vous pouvez utiliser la fonctionnalité de connexion de la console Developer Tools pour connecter AWS des ressources telles que AWS CodePipeline des référentiels de code externes. Cette fonctionnalité possède sa propre API, la référence de l'API AWS CodeStar Connections. Chaque connexion est une ressource que vous pouvez attribuer à AWS des services pour qu'ils se connectent à un référentiel tiers, tel que BitBucket. Par exemple, vous pouvez ajouter la connexion CodePipeline afin qu'elle déclenche votre pipeline lorsqu'une modification de code est apportée à votre référentiel de code tiers. Chaque connexion est nommée et associée à un Amazon Resource Name (ARN) unique utilisé pour référencer la connexion.

Que puis-je faire avec les connexions ?

Vous pouvez utiliser des connexions pour intégrer des ressources de fournisseurs tiers à vos ressources AWS dans des outils pour développeurs, notamment :

- Connectez-vous à un fournisseur tiers, tel que Bitbucket, et utilisez la connexion tierce comme source d'intégration à vos AWS ressources, par exemple. CodePipeline

- Gérez de manière uniforme l'accès à votre connexion sur l'ensemble de vos ressources lors de la CodeBuild création de projets, d' CodeDeploy applications et de pipelines CodePipeline pour le compte de votre fournisseur tiers.
- Utilisez un ARN de connexion dans vos modèles de pile pour CodeBuild créer des projets, CodeDeploy des applications et des pipelines CodePipeline, sans avoir à faire référence à des secrets ou à des paramètres stockés.

Pour quels fournisseurs tiers puis-je créer des connexions ?

Les connexions peuvent associer vos AWS ressources aux référentiels tiers suivants :

- Bitbucket Cloud
- GitHub
- GitHub Cloud d'entreprise
- GitHub Serveur d'entreprise
- GitLab
- GitLab installation autogérée (pour Enterprise Edition ou Community Edition)

Pour obtenir une présentation du flux de travail des connexions, veuillez consulter Flux de travail permettant de créer ou de mettre à jour des connexions.

Les étapes de création de connexions pour un type de fournisseur de cloud GitHub, tel que, sont différentes des étapes pour un type de fournisseur installé, tel que GitHub Enterprise Server. Pour connaître les étapes de haut niveau de création d'une connexion par type de fournisseur, consultez Utilisation des connexions.

> **Note**
>
> Pour utiliser les connexions en Europe (Milan) Région AWS, vous devez :
>
> 1. Installer une application spécifique à la région
> 2. Activer la région
>
> Cette application spécifique à la région prend en charge les connexions dans la région Europe (Milan). Elle est publiée sur le site du fournisseur tiers et est distincte de l'application

existante qui prend en charge les connexions pour d'autres régions. En installant cette application, vous autorisez les fournisseurs tiers à partager vos données avec le service pour cette région uniquement et vous pouvez révoquer les autorisations à tout moment en désinstallant l'application.
Le service ne traitera ni ne stockera vos données à moins que vous n'activiez la région. En activant cette région, vous autorisez notre service à traiter et à stocker vos données.
Même si la région n'est pas activée, les fournisseurs tiers peuvent toujours partager vos données avec notre service si l'application spécifique à la région reste installée. Veillez donc à désinstaller l'application une fois que vous avez désactivé la région. Pour plus d'informations, consultez Activer une région.

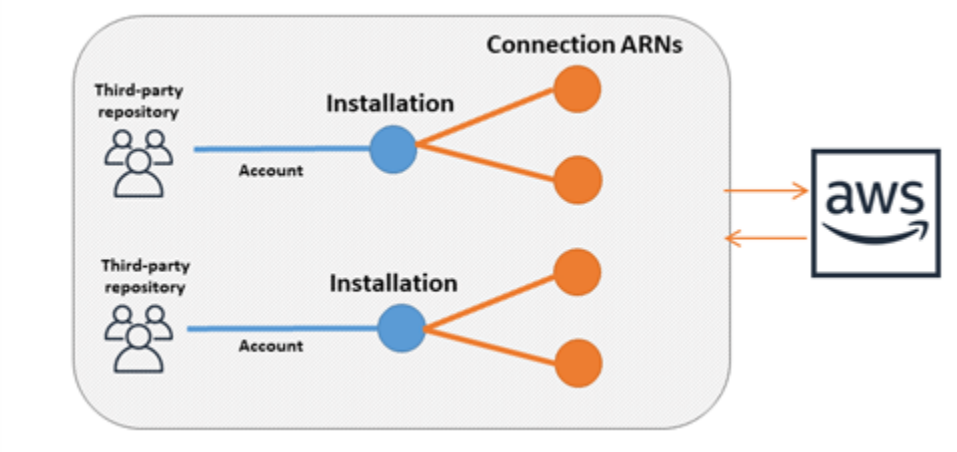
Qu'est-ce qui Services AWS s'intègre aux connexions ?

Vous pouvez utiliser des connexions pour intégrer votre référentiel tiers avec d'autres Services AWS. Pour consulter les intégrations de services pour les connexions, consultez Intégrations de produits et services à AWS CodeStar Connections.

Comment fonctionnent les connexions ?

Avant de pouvoir créer une connexion, vous devez d'abord installer ou fournir un accès à l'application d'authentification AWS sur votre compte tiers. Une fois qu'une connexion est installée, elle peut être mise à jour pour utiliser cette installation. Lorsque vous créez une connexion, vous fournissez l'accès à la ressource AWS dans votre compte tiers. Cela permet à la connexion d'accéder au contenu, tel que les référentiels sources, dans le compte tiers, au nom de vos AWS ressources. Vous pouvez ensuite partager cette connexion avec d'autres personnes Services AWS pour fournir des connexions OAuth sécurisées entre les ressources.

Si vous souhaitez créer une connexion à un type de fournisseur installé, tel que GitHub Enterprise Server, vous devez d'abord créer une ressource hôte à l'aide du AWS Management Console.



Les connexions appartiennent à celui Compte AWS qui les crée. Les connexions sont identifiées par un ARN contenant un ID de connexion. L'ID de connexion est un UUID qui ne peut pas être modifié ou remappé. La suppression et le rétablissement d'une connexion entraînent un nouvel ID de connexion, et donc un nouvel ARN de connexion. Cela signifie que les ARN de connexion ne sont jamais réutilisés.

Une connexion nouvellement créée présente l'état `Pending`. Un processus de négociation tierce (flux OAuth) est nécessaire pour terminer la configuration de la connexion et pour qu'elle passe de l'état `Pending` à l'état `Available`. Une fois cette opération terminée, une connexion est `Available` et peut être utilisée avec AWS des services tels que CodePipeline.

Un hôte nouvellement créé présent l'état `Pending`. Un processus d'enregistrement tiers est nécessaire pour terminer la configuration de l'hôte et pour qu'il passe de l'état `Pending` à l'état `Available`. Une fois cette opération terminée, un hôte est `Available` et peut être utilisé pour les connexions aux types de fournisseurs installés.

Pour obtenir une présentation du flux de travail des connexions, veuillez consulter Flux de travail permettant de créer ou de mettre à jour des connexions. Pour voir une présentation du flux de travail de création d'hôte pour les fournisseurs installés, consultez Flux de travail de création ou de mise à jour d'un hôte. Pour connaître les étapes de haut niveau de création d'une connexion par type de fournisseur, consultez Utilisation des connexions.

Ressources mondiales dans AWS CodeStar Connections

Les connexions sont des ressources globales, ce qui signifie que la ressource est répliquée dans toutes les Régions AWS.

Bien que le format ARN de connexion reflète le nom de la région dans laquelle elle a été créée, la ressource n'est soumise à aucune région. La région dans laquelle la ressource de connexion a été créée est la région où les mises à jour des données de ressource de connexion sont contrôlées. Des exemples d'opérations d'API qui contrôlent les mises à jour des données de ressource de connexion incluent la création d'une connexion, la mise à jour d'une installation, la suppression d'une connexion ou le balisage d'une connexion.

Les ressources hôtes pour les connexions ne sont pas des ressources disponibles globalement. Vous utilisez les ressources hôtes uniquement dans la région où elles ont été créées.

- Vous n'avez qu'à créer une connexion qu'une seule fois, puis vous pouvez l'utiliser dans n'importe quelle Région AWS.
- Si la région dans laquelle la connexion a été créée rencontre des problèmes, cela affecte les API qui contrôlent les données de ressource de connexion, mais vous pouvez continuer à utiliser la connexion dans toutes les autres régions.
- Lorsque vous répertoriez les ressources de connexion dans la console ou la CLI, la liste affiche toutes les ressources de connexion associées à votre compte dans toutes les régions.
- Lorsque vous répertoriez les ressources hôtes dans la console ou la CLI, la liste affiche toutes les ressources hôtes associées à votre compte dans toutes les régions sélectionnées.
- Lorsqu'une connexion avec une ressource hôte associée est répertoriée ou affichée avec la CLI, la sortie renvoie l'ARN hôte quelle que soit la région CLI configurée.

Flux de travail de création ou de mise à jour d'un hôte

Lorsque vous créez une connexion pour un fournisseur installé, vous devez d'abord créer un hôte.

Les hôtes peuvent avoir les états suivants :

- `Pending` : un hôte à l'état `pending` est un hôte qui a été créé et qui doit être configuré (passé à l'état `available`) avant de pouvoir être utilisé.
- `Available` : vous pouvez utiliser ou transférer un hôte `available` à votre connexion.

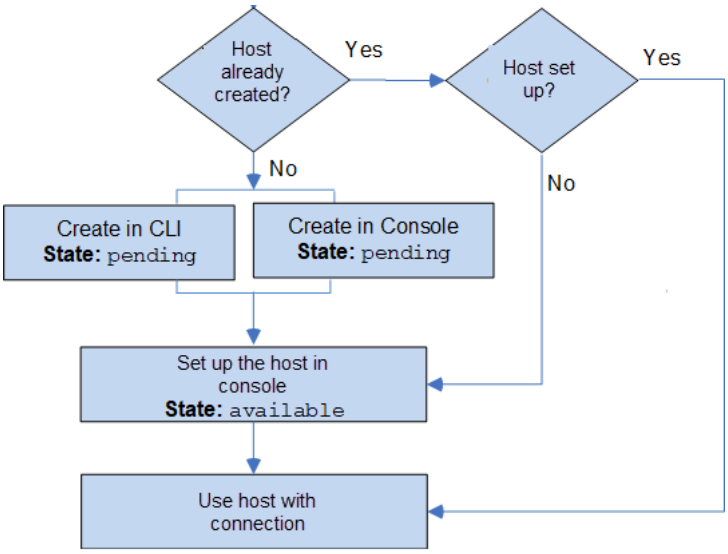
Flux de travail : création ou mise à jour d'un hôte avec la CLI, le kit SDK ou AWS CloudFormation

Vous utilisez l'CreateHostAPI pour créer un hôte à l'aide du AWS Command Line Interface (AWS CLI), du SDK ou AWS CloudFormation. Une fois créé, l'hôte est à l'état `pending`. Vous effectuez le processus à l'aide de l'option Configuration de la console.

Flux de travail : création ou mise à jour d'un hôte avec la console

Si vous créez une connexion avec un type de fournisseur installé, tel qu'un serveur GitHub d'entreprise ou un fournisseur GitLab autogéré, vous devez d'abord créer un hôte. Si vous vous connectez à un type de fournisseur de cloud, tel que Bitbucket, ignorez la création de l'hôte et continuez à créer une connexion.

Utilisez la console pour configurer l'hôte et le faire passer de l'état `pending` à `available`.



Flux de travail permettant de créer ou de mettre à jour des connexions

Lorsque vous créez une connexion, vous créez ou utilisez également une installation existante pour la négociation d'authentification avec le fournisseur tiers.

Les états des connexions peuvent être les suivants :

- `Pending` - Une connexion `pending` est une connexion qui doit être établie (déplacée vers `available`) avant de pouvoir être utilisée.
- `Available` - Vous pouvez utiliser ou transférer une connexion `available` vers d'autres ressources et utilisateurs dans votre compte.
- `Error` - Une connexion qui présente un état `error` est automatiquement retentée. Elle ne peut pas être utilisée tant qu'elle ne présente pas l'état `available`.

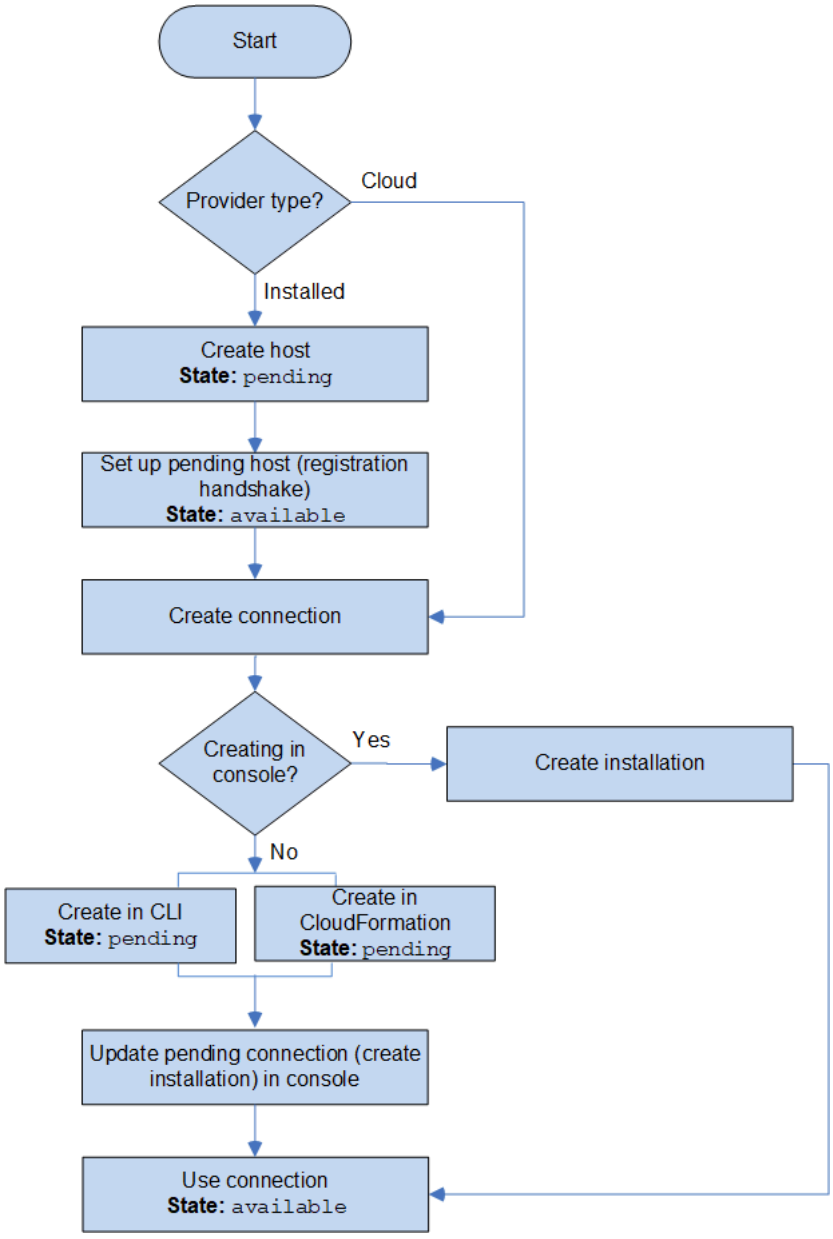
Flux de travail : création ou mise à jour d'une connexion avec la CLI, le kit SDK ou AWS CloudFormation

Vous utilisez l'CreateConnectionAPI pour créer une connexion à l'aide du AWS Command Line Interface (AWS CLI), du SDK ou AWS CloudFormation. Une fois qu'elle est créée, la connexion présente l'état `pending`. Vous terminez le processus à l'aide de l'option de console Configuration d'une connexion en attente. La console vous invite à créer une installation ou à utiliser une installation existante pour la connexion. Vous utilisez ensuite la console pour terminer la négociation et déplacer la connexion vers un état `available` en choisissant Établir la connexion sur la console.

Flux de travail : création ou mise à jour d'une connexion avec la console

Si vous créez une connexion avec un type de fournisseur installé, tel que GitHub Enterprise Server, vous devez d'abord créer un hôte. Si vous vous connectez à un type de fournisseur de cloud, tel que Bitbucket, ignorez la création de l'hôte et continuez à créer une connexion.

Pour créer ou mettre à jour une connexion à l'aide de la console, vous devez utiliser la page d'action de CodePipeline modification de la console pour choisir votre fournisseur tiers. La console vous invite à créer une installation ou à utiliser une installation existante pour la connexion, puis à utiliser la console pour créer la connexion. La console termine la négociation et déplace automatiquement la connexion de l'état `pending` à l'état `available`.



Comment démarrer avec les connexions ?

Pour commencer, voici quelques rubriques utiles à consulter :

- Découvrez les concepts des connexions.
- Configurez les ressources dont vous avez besoin pour commencer à utiliser les connexions.
- Démarrez avec vos premières connexions et connectez-les à une ressource.

Concepts de connexion

Vous trouverez la configuration et l'utilisation des fonctions de connexion plus simples si vous comprenez les concepts et les termes. Voici quelques concepts à connaître lorsque vous utilisez les connexions dans la console Outils pour développeurs :

installation

Une instance de l'appli AWS sur un compte tiers. L'installation de l'application AWS CodeStar Connector permet à AWS d'accéder à des ressources dans le compte tiers. Une installation ne peut être modifiée que sur le site Web du fournisseur tiers.

connexion

Un ressource AWS utilisée pour connecter des référentiels sources tiers à d'autres services AWS.

référentiel tiers

Un référentiel fourni par un service ou une société qui ne fait pas partie de AWS. Par exemple, un référentiel BitBucket est un référentiel tiers.

type de fournisseur

Un service ou une société qui fournit le référentiel source tiers auquel vous souhaitez vous connecter. Vous connectez vos ressources AWS aux types de fournisseurs externes. Un type de fournisseur dans lequel le référentiel source est installé sur le réseau et l'infrastructure est un type de fournisseur installé. Par exemple, GitHub Enterprise Server est un type de fournisseur installé.

hôte

Une ressource qui représente l'infrastructure sur laquelle un fournisseur tiers est installé. Les connexions utilisent l'hôte pour représenter le serveur sur lequel votre fournisseur tiers est installé, tel que GitHub Enterprise Server. Vous créez un hôte pour toutes les connexions vers ce type de fournisseur.

> **Note**
>
> Lorsque vous utilisez la console pour créer une connexion à GitHub Enterprise Server, la console crée une ressource hôte pour vous dans le cadre du processus.

AWS CodeStar Connexions, fournisseurs et versions pris en charge

Ce chapitre fournit des informations sur les fournisseurs et les versions pris en charge par AWS CodeStar Connections.

Rubriques

Type de fournisseur pris en charge pour Bitbucket

Vous pouvez utiliser l' AWS CodeStar application avec Atlassian Bitbucket Cloud.

Les types de fournisseurs Bitbucket installés, tels que Bitbucket Server, ne sont pas pris en charge.

Type de fournisseur pris en charge pour GitHub et GitHub Enterprise Cloud

Vous pouvez utiliser le AWS Connector pour une GitHub application avec GitHub GitHub Enterprise Cloud.

Type de fournisseur et versions pris en charge pour GitHub Enterprise Server

Vous pouvez utiliser l' AWS CodeStar application avec les versions prises en charge d' GitHub Enterprise Server. Pour une liste de versions prises en charge, consultez https://enterprise.github.com/releases/.

> **Important**
>
> AWS CodeStar Connections ne prend pas en charge les versions obsolètes GitHub d'Enterprise Server. Par exemple, AWS CodeStar Connections ne prend pas en charge la version 2.22.0 d' GitHub Enterprise Server en raison d'un problème connu dans cette version. Pour vous connecter, effectuez une mise à niveau vers la version 2.22.1 ou vers la dernière version disponible.

Type de fournisseur pris en charge pour GitLab

Vous pouvez utiliser des connexions avec GitLab. Pour plus d'informations, consultez Créez une connexion avec GitLab.

Type de fournisseur pris en charge pour l' GitLab autogestion

Vous pouvez utiliser des connexions avec une installation GitLab autogérée (pour Enterprise Edition ou Community Edition). Pour plus d'informations, voir Création d'une connexion à l' GitLabautogestion.

Intégrations de produits et services à AWS CodeStar Connections

AWS CodeStar Connections est intégré à plusieurs services AWS, ainsi qu'à des produits et services partenaires. Utilisez les informations indiquées dans les sections suivantes pour vous aider à configurer Connections pour l'intégrer aux produits et services que vous utilisez.

Les ressources connexes suivantes peuvent s'avérer utiles lors de l'utilisation de ce service.

Rubriques

- Amazon CodeGuru Reviewer
- Amazon CodeWhisperer
- Amazon SageMaker
- AWS App Runner
- AWS CloudFormation
- AWS CodePipeline
- AWS CodeStar
- Service Catalog
- AWS Proton

Amazon CodeGuru Reviewer

CodeGuru Reviewer est un service de surveillance du code de votre dépôt. Vous pouvez utiliser des connexions pour associer le référentiel tiers contenant le code à afficher. Pour un didacticiel dans lequel vous apprendrez à configurer CodeGuru Reviewer pour surveiller le code source dans un

référentiel GitHub afin de créer des recommandations visant à améliorer le code, consultez Tutoriel : surveiller le code source dans un dépôt GitHub dans le Guide de l'utilisateur Amazon CodeGuru Reviewer.

Amazon CodeWhisperer

Amazon CodeWhisperer est un service dont vous pouvez vous servir pour vérifier votre code de référentiel. CodeWhisperer vérifie votre code et vous adresse en temps réel des recommandations en matière de code. Pour savoir comment configurer une personnalisation dans CodeWhisperer étape par étape qui vous permet d'accéder à la source de données à l'aide d'une connexion, consultez Création de votre personnalisation dans le Guide de l'utilisateur Amazon CodeWhisperer.

Amazon SageMaker

Amazon SageMaker est un service de création, d'apprentissage et de déploiement de modèles de langage de machine learning. Pour accéder à un didacticiel dans lequel vous configurez une connexion à votre référentiel GitHub, consultez Procédure pas à pas du projet SageMaker MLOps en utilisant des référentiels Git tiers dans le Guide du développeur Amazon SageMaker.

AWS App Runner

AWS App Runner est un service qui offre un moyen rapide, simple et économique de déployer directement, à partir du code source ou d'une image de conteneur, une application web évolutive et sécurisée dans le AWS Cloud. Vous pouvez déployer du code d'application depuis votre référentiel grâce à un pipeline d'intégration et de diffusion automatique d'App Runner. Vous pouvez utiliser des connexions pour déployer votre code source vers un service App Runner à partir d'un référentiel GitHub privé. Pour plus d'informations, veuillez consulter la rubrique Fournisseurs de référentiel de code source dans le Manuel du développeur AWS App Runner.

AWS CloudFormation

AWS CloudFormation est un service qui vous permet de modéliser et de configurer vos ressources AWS de sorte que vous puissiez passer moins de temps à gérer ces ressources et consacrer plus de temps à vos applications exécutées dans AWS. Vous créez un modèle qui décrit toutes les ressources AWS que vous voulez (telles que des instances Amazon EC2 ou des instances de base de données Amazon RDS), et CloudFormation s'occupe de leur allocation et de leur configuration. Pour plus d'informations, veuillez consulter la rubrique Enregistrement de votre compte pour publier des extensions CloudFormation dans le Guide de l'utilisateur de l'interface de ligne de commande CloudFormation.

AWS CodePipeline

CodePipeline est un service de diffusion continue qui vous permet de modéliser, de visualiser et d'automatiser les étapes nécessaires à la publication de votre logiciel. Vous pouvez utiliser des connexions pour configurer un référentiel tiers pour les actions source CodePipeline.

En savoir plus :

- Consultez la page de référence de configuration de l'action CodePipeline pour l'action `CodeStarSourceConnection`. Pour consulter les paramètres de configuration et un exemple de fragment de code JSON/YAML, consultez CodeStarSourceConnection dans le Guide de l'utilisateur AWS CodePipeline.
- Pour afficher un didacticiel Démarrage qui crée un pipeline avec un référentiel source tiers, consultez Mise en route avec les connexions.

AWS CodeStar

AWS CodeStar est un service basé sur le cloud qui permet de créer, gérer et utiliser des projets de développement logiciel sur AWS. Vous pouvez développer, créer et déployer rapidement des applications sur AWS via un projet AWS CodeStar. Vous pouvez utiliser des connexions pour configurer vos référentiels tiers pour les pipelines de vos projets AWS CodeStar. Pour accéder à un didacticiel dans lequel vous créez un projet AWS CodeStar avec une connexion à un référentiel GitHub, consultez Création d'un lien vers votre référentiel dans le Guide de l'utilisateur AWS CodeStar.

Service Catalog

Service Catalog permet aux organisations de créer et de gérer des catalogues de produits qui sont approuvés pour être utilisés sur AWS.

Lorsque vous autorisez une connexion entre votre Compte AWS et un fournisseur de référentiel externe, tel que GitHub, GitHub Enterprise ou BitBucket, la connexion vous permet de synchroniser les produits Service Catalog avec des fichiers modèles gérés via des référentiels tiers.

Pour plus d'informations, consultez Synchronisation des produits Service Catalog avec des modèles de fichiers de GitHub, de GitHub Enterprise ou de Bitbucket dans le Guide de l'utilisateur de Service Catalog.

AWS Proton

AWS Proton est un service basé sur le cloud destiné à être déployé sur une infrastructure cloud. Vous pouvez utiliser des connexions pour créer un lien vers vos référentiels tiers pour les ressources de vos modèles pour AWS Proton. Pour plus d'informations, veuillez consulter la rubrique Créer un lien vers votre référentiel dans le Guide de l'utilisateur AWS Proton.

Configuration de connexions

Effectuez les tâches décrites dans cette section pour configurer la création et l'utilisation de la fonction de connexion dans la console Outils pour développeurs.

Rubriques

- Inscrivez-vous à AWS
- Création et application d'une politique avec des autorisations pour créer des connexions

Inscrivez-vous à AWS

Ouverture d'un Compte AWS

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

Pour ouvrir un Compte AWS

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

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

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

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

Création d'un utilisateur administratif

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

Sécurisation de votre Utilisateur racine d'un compte AWS

1. Connectez-vous à la AWS Management Console en tant que propriétaire du compte en sélectionnant Utilisateur root et en saisissant l'adresse e-mail de votre Compte AWS. Sur la page suivante, saisissez votre mot de passe.

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

   Pour obtenir des instructions, consultez Activation d'un dispositif MFA virtuel pour l'utilisateur root de votre Compte AWS (console) dans le Guide de l'utilisateur IAM.

Création d'un utilisateur administratif

1. Activez IAM Identity Center.

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

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

Connexion en tant qu'utilisateur administratif

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

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

Création et application d'une politique avec des autorisations pour créer des connexions

Pour utiliser l'éditeur de politique JSON afin de créer une politique

1. Connectez-vous à la AWS Management Console et ouvrez la console IAM à l'adresse https://console.aws.amazon.com/iam/.
2. Dans le panneau de navigation de gauche, sélectionnez Policies (Politiques).

   Si vous sélectionnez Politiques pour la première fois, la page Bienvenue dans les politiques gérées s'affiche. Sélectionnez Mise en route.
3. En haut de la page, sélectionnez Créer une politique.
4. Dans la section Éditeur de politiques, choisissez l'option JSON.
5. Entrez le document de politique JSON suivant :

```
{
   "Version": "2012-10-17",
   "Statement": [
       {
           "Effect": "Allow",
           "Action": [
               "codestar-connections:CreateConnection",
               "codestar-connections:DeleteConnection",
               "codestar-connections:GetConnection",
               "codestar-connections:ListConnections",
               "codestar-connections:GetInstallationUrl",
               "codestar-connections:GetIndividualAccessToken",
               "codestar-connections:ListInstallationTargets",
               "codestar-connections:StartOAuthHandshake",
               "codestar-connections:UpdateConnectionInstallation",
               "codestar-connections:UseConnection"
           ],
           "Resource": [
               "*"
           ]
       }
   ]
}
```

6. Choisissez Next (Suivant).

> **Note**
>
> Vous pouvez basculer à tout moment entre les options des éditeurs visuel et JSON. Toutefois, si vous apportez des modifications ou si vous choisissez Suivant dans l'éditeur visuel, IAM peut restructurer votre politique afin de l'optimiser pour l'éditeur visuel. Pour de plus amples informations, consulte Restructuration d'une politique dans le Guide de l'utilisateur IAM.

7. Sur la page Vérifier et créer, saisissez un Nom de politique et une Description (facultative) pour la politique que vous créez. Vérifiez les Autorisations définies dans cette politique pour voir les autorisations accordées par votre politique.
8. Choisissez Create policy (Créer une politique) pour enregistrer votre nouvelle politique.

Mise en route avec les connexions

Le moyen le plus simple de commencer à utiliser les connexions consiste à configurer une connexion qui associe votre référentiel source tiers à vos ressources AWS. Si vous souhaitez connecter votre pipeline à une source AWS, telle que CodeCommit, vous vous y connecteriez en tant qu'action source. Toutefois, si vous disposez d'un référentiel externe, vous devez créer une connexion pour associer votre référentiel à votre pipeline. Dans ce didacticiel, vous configurez une connexion avec votre référentiel Bitbucket et votre pipeline.

Dans cette section, vous utilisez des connexions avec :

- AWS CodePipeline : dans ces étapes, vous créez un pipeline avec votre référentiel Bitbucket comme source de pipeline.
- Amazon CodeGuru Reviewer : associez ensuite votre référentiel Bitbucket à vos outils de commentaires et d'analyses dans CodeGuru Reviewer.

Rubriques

Prérequis

Avant de commencer, complétez les étapes détaillées dans Configuration. Vous avez également besoin d'un référentiel source tiers que vous souhaitez connecter à vos services AWS et autoriser la connexion à gérer l'authentification pour vous. Par exemple, vous pouvez connecter un référentiel Bitbucket à vos services AWS qui s'intègrent aux référentiels sources.

- Créez un référentiel Bitbucket avec votre compte Bitbucket.
- Préparez vos informations d'identification Bitbucket. Lorsque vous utilisez la AWS Management Console pour configurer une connexion, vous êtes invité à vous connecter avec vos informations d'identification Bitbucket.

Étape 1 : Modifier votre fichier source

Lorsque vous créez votre référentiel Bitbucket, un fichier `README.md` par défaut est inclus, que vous allez modifier.

1. Connectez-vous à votre référentiel Bitbucket et choisissez Source.
2. Choisissez le fichier `README.md` et choisissez Edit (Modifier) en haut de la page. Supprimez le texte existant et ajoutez le texte suivant.

   ```
   This is a Bitbucket repository!
   ```

3. Choisissez Commit (Valider).

   Assurez-vous que le fichier `README.md` est au niveau racine de votre référentiel.

Étape 2 : Créer votre pipeline

Dans cette section, vous créez un pipeline avec les actions suivantes :

- Étape source avec une connexion à votre référentiel et action Bitbucket.
- Une étape de génération avec une action de génération AWS CodeBuild.

Pour créer un pipeline avec l'assistant

1. Connectez-vous à la console CodePipeline via https://console.aws.amazon.com/codepipeline/.
2. Sur la page Bienvenue, Démarrez ou Pipelines, choisissez Créer un pipeline.

3. Dans l'Étape 1 : Choisir les paramètres d'un pipeline, dans Nom du pipeline, saisissez **`MyBitbucketPipeline`**.
4. Dans Service role (Rôle de service), choisissez New service role (Nouveau rôle de service).

   > **Note**
   >
   > Si vous choisissez plutôt d'utiliser votre rôle de service CodePipeline existant, assurez-vous d'avoir ajouté l'autorisation IAM `codestar-connections:UseConnection` à votre stratégie de rôle de service. Pour obtenir des instructions sur le rôle de service, consultez Ajouter des autorisations au rôle de service CodePipeline.

5. Sous Paramètres avancés, conservez les valeurs par défaut. Dans le magasin d'artefacts choisissez Default location (Emplacement par défaut) pour utiliser le magasin d'artefacts par défaut, tel que le compartiment d'artefacts Amazon S3 désigné par défaut, pour votre pipeline dans la région que vous avez sélectionnée pour ce dernier.

   > **Note**
   >
   > Il ne s'agit pas du compartiment source de votre code source. Il s'agit du magasin d'artefacts pour votre pipeline. Un magasin d'artefacts distinct, tel qu'un compartiment S3, est nécessaire pour chaque pipeline.

   Choisissez Next (Suivant).
6. Sur la page Étape 2 : Ajouter une étape source, ajoutez un étape source :

   a. Dans Source provider (Fournisseur de source), choisissez Bitbucket.

   b. Sous Connection (Connexion), choisissez Connect to Bitbucket (Connexion à Bitbucket).

   c. Sur la page Se connecter à Bitbucket, dans Connection name (Nom de la connexion), saisissez le nom de la connexion que vous souhaitez créer. Ce nom vous permettra d'identifier cette connexion ultérieurement.

      Sous Bitbicket apps (Applications BitBucket), choisissez Install a new app (Installer une nouvelle application).

   d. Sur la page d'installation de l'application, un message indique que l'application AWS CodeStar tente de se connecter à votre compte Bitbucket. Choisissez Grant access

(Accorder l'accès). Après avoir autorisé la connexion, vos référentiels sur Bitbucket sont détectés et vous pouvez choisir d'en associer un à votre ressource AWS.

e. L'ID de connexion de votre nouvelle installation s'affiche. Choisissez Complete connection (Terminer la connexion). Vous serez redirigé vers la console CodePipeline.

f. Dans Repository name (Nom du référentiel), choisissez le nom de votre référentiel Bitbucket.

g. Dans Branch name (Nom de la branche), choisissez la branche de votre référentiel.

h. Veillez à ce que l'option Démarrer le pipeline lors de la modification du code source soit sélectionnée.

i. Sous Format d'artefact de sortie, choisissez l'une des options suivantes : CodePipeline par défaut.

- Choisissez CodePipeline par défaut pour utiliser le format zip par défaut pour les artefacts du pipeline.
- Choisissez Clone complet pour inclure les métadonnées Git relatives au référentiel d'artefacts dans le pipeline. Ceci n'est pris en charge que pour les actions CodeBuild.

Choisissez Next (Suivant).

7. Dans le champ Ajouter une étape de génération, ajoutez une étape de génération :

a. Dans le champ Fournisseur de génération, choisissez AWS CodeBuild. Acceptez la région du pipeline comme Région par défaut.

b. Sélectionnez Create a project (Créer un projet).

c. Dans Nom du projet, saisissez un nom pour ce projet de génération.

d. Dans le champ Image d'environnement, choisissez Image gérée. Pour Système d'exploitation, choisissez Ubuntu.

e. Pour Runtime (Exécution), sélectionnez Standard. Pour Image, choisissez aws/codebuild/standard:5.0.

f. Pour Rôle de service, choisissez Nouveau rôle de service.

g. Sous Buildspec, pour Build specifications (Spécifications de génération), choisissez Insert build commands (Insérer des commandes de génération). Choisissez Switch to editor (Passer à l'éditeur), et collez ce qui suit sous Build commands (Commandes de génération) :

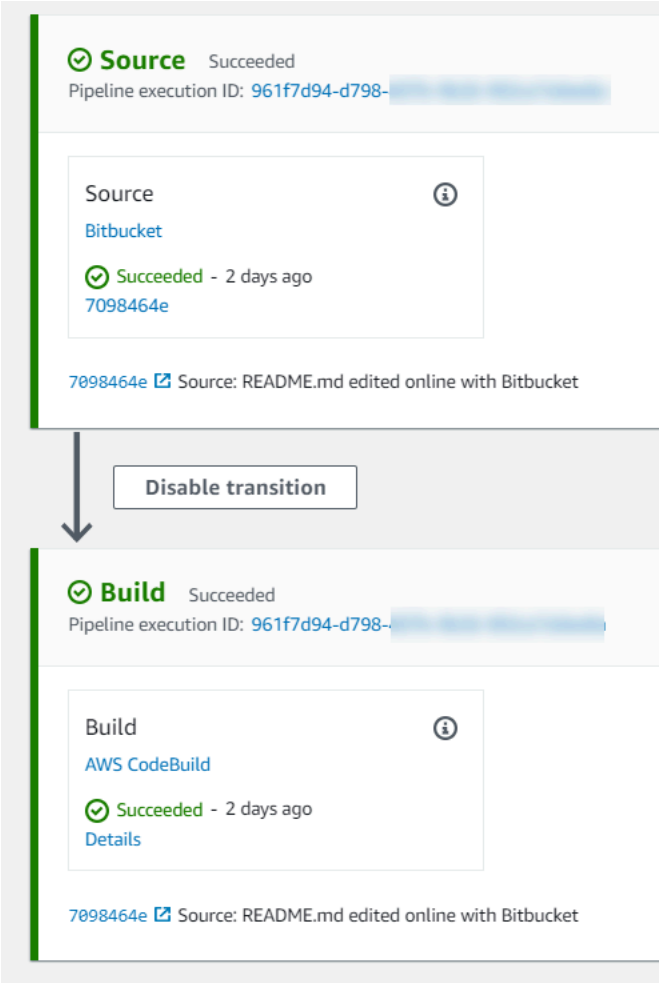
```
version: 0.2
```

```
phases:
  install:
    #If you use the Ubuntu standard image 2.0 or later, you must specify
 runtime-versions.
    #If you specify runtime-versions and use an image other than Ubuntu
 standard image 2.0, the build fails.
    runtime-versions:
      nodejs: 12
      # name: version
    #commands:
      # - command
      # - command
  pre_build:
    commands:
      - ls -lt
      - cat README.md
  # build:
    #commands:
      # - command
      # - command
  #post_build:
    #commands:
      # - command
      # - command
#artifacts:
  #files:
    # - location
    # - location
  #name: $(date +%Y-%m-%d)
  #discard-paths: yes
  #base-directory: location
#cache:
  #paths:
    # - paths
```

h. Choisissez Continue to CodePipeline (Poursuivre avec CodePipeline). Ceci permet de revenir à la console CodePipeline et de créer un projet CodeBuild qui utilise vos commandes de génération pour la configuration. Le projet de génération utilise un rôle de service pour gérer les autorisations des services AWS. Cette étape peut prendre quelques minutes.

i. Choisissez Next (Suivant).

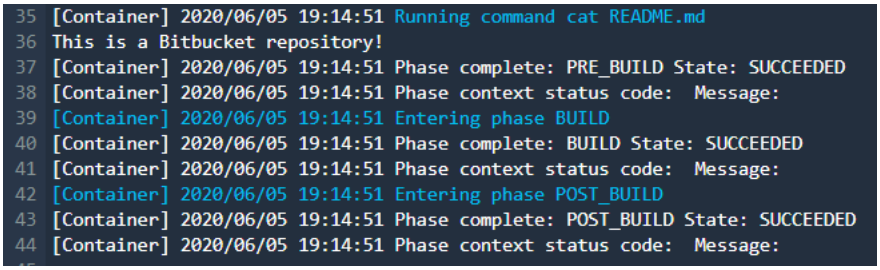
8. Sur la page Step 4: Add deploy stage (Étape 4 : Ajouter une étape de déploiement), choisissez Skip deploy stage (Ignorer l'étape de déploiement), puis acceptez le message d'avertissement en choisissant à nouveau Skip (Ignorer). Choisissez Next (Suivant).
9. Dans Étape 5 : Vérification, choisissez Créer un pipeline.
10. Lorsque votre pipeline est créé avec succès, une exécution de pipeline démarre.



11. Lorsque votre phase de génération est réussie, choisissez Details (Détails).

    Sous Execution details (Détails de l'exécution), affichez la sortie de génération CodeBuild. Les commandes génèrent le contenu du fichier `README.md` comme suit :

```
This is a Bitbucket repository!
```



Étape 3 : Associer votre référentiel à CodeGuru Reviewer

Après avoir créé une connexion, vous pouvez utiliser cette connexion pour toutes vos ressources AWS dans le même compte. Par exemple, vous pouvez utiliser la même connexion Bitbucket pour une action source CodePipeline dans un pipeline et votre analyse de validation de référentiel dans CodeGuru Reviewer.

1. Connectez-vous à la console CodeGuru Reviewer.
2. Sous CodeGuru Reviewer, choisissez Associate repository (Associer un référentiel).

   L'assistant sur une page s'ouvre.
3. Sous Select source provider (Sélectionner le fournisseur source), choisissez Bitbucket.
4. Sous Connect to Bitbucket (with AWS CodeStar connections) (Se connecter à Bitbucket (avec AWS CodeStar Connections)), choisissez la connexion que vous avez créée pour votre pipeline.
5. Sous Repository location (Emplacement du référentiel), choisissez le nom de votre référentiel Bitbucket et choisissez Associate (Associer).

   Vous pouvez continuer à configurer les révisions de code. Pour de plus amples informations, veuillez consulter Connexion à Bitbucket pour associer un référentiel à CodeGuru Reviewer dans le guide de l'utilisateur Amazon CodeGuru Reviewer.

Utilisation des connexions

Les connexions sont des configurations que vous utilisez pour connecter des ressources AWS à des référentiels de code externes. Chaque connexion est une ressource qui peut être attribuée à des services tels que AWS CodePipeline la connexion à un référentiel tiers tel que Bitbucket. Par exemple, vous pouvez ajouter la connexion CodePipeline afin qu'elle déclenche votre pipeline lorsqu'une modification de code est apportée à votre référentiel de code tiers. Vous pouvez

également connecter vos AWS ressources à un type de fournisseur installé tel que GitHub Enterprise Server.

Si vous souhaitez créer une connexion avec un type de fournisseur installé, tel que GitHub Enterprise Server, la console crée un hôte pour vous. Un hôte est une ressource que vous créez pour représenter le serveur sur lequel votre fournisseur est installé. Pour plus d'informations, consultez Utilisation d'hôtes.

Lorsque vous créez une connexion, vous utilisez un assistant de la console pour installer l' AWS CodeStar application auprès de votre fournisseur tiers et l'associer à une nouvelle connexion. Si vous avez déjà installé l' AWS CodeStar application, vous pouvez l'utiliser.

> **Note**
>
> Pour utiliser les connexions en Europe (Milan) Région AWS, vous devez :
>
> 1. Installer une application spécifique à la région
> 2. Activer la région
>
> Cette application spécifique à la région prend en charge les connexions dans la région Europe (Milan). Elle est publiée sur le site du fournisseur tiers et est distincte de l'application existante qui prend en charge les connexions pour d'autres régions. En installant cette application, vous autorisez les fournisseurs tiers à partager vos données avec le service pour cette région uniquement et vous pouvez révoquer les autorisations à tout moment en désinstallant l'application.
> Le service ne traitera ni ne stockera vos données à moins que vous n'activiez la région. En activant cette région, vous autorisez notre service à traiter et à stocker vos données.
> Même si la région n'est pas activée, les fournisseurs tiers peuvent toujours partager vos données avec notre service si l'application spécifique à la région reste installée. Veillez donc à désinstaller l'application une fois que vous avez désactivé la région. Pour plus d'informations, consultez Activer une région.

Pour plus d'informations sur les connexions, consultez la référence de l'API AWS CodeStar Connections. Pour plus d'informations sur l'action CodePipeline source pour Bitbucket, consultez le guide CodestarConnectionSourcede l'AWS CodePipeline utilisateur.

Pour créer ou associer une politique à votre utilisateur ou à votre rôle AWS Identity and Access Management (IAM) avec les autorisations requises pour utiliser AWS CodeStar les connexions, consultezAWS CodeConnections référence aux autorisations. En fonction de la date de création de votre rôle de CodePipeline service, vous devrez peut-être mettre à jour ses autorisations pour prendre en charge AWS CodeStar les connexions. Pour obtenir des instructions, consultez Mettre à jour le rôle de service dans le guide de l'utilisateur AWS CodePipeline .

Rubriques

Créez une connexion

Vous pouvez créer des connexions aux types de fournisseurs tiers suivants :

- Pour créer une connexion à Bitbucket, consultez Créer une connexion à Bitbucket.
- Pour créer une connexion à Enterprise Cloud GitHub ou à GitHub Enterprise Cloud, consultezCréez une connexion avec GitHub.
- Pour créer une connexion à GitHub Enterprise Server, notamment pour créer votre ressource hôte, consultezCréation d'une connexion à GitHub Enterprise Server.
- Pour créer une connexion à GitLab, voirCréez une connexion avec GitLab.

Créer une connexion à Bitbucket

Vous pouvez utiliser le AWS Management Console ou le AWS Command Line Interface (AWS CLI) pour créer une connexion à un dépôt hébergé sur bitbucket.org.

Avant de commencer :

- Vous devez déjà avoir créé un compte avec Bitbucket.
- Vous devez déjà avoir créé un référentiel de code sur bitbucket.org.

> **Note**
>
> Vous pouvez créer des connexions à un référentiel Bitbucket Cloud. Les types de fournisseurs Bitbucket installés, tels que Bitbucket Server, ne sont pas pris en charge. Voir AWS CodeStar Connexions, fournisseurs et versions pris en charge.

> **Note**
>
> Les connexions fournissent uniquement l'accès aux référentiels appartenant au compte qui a été utilisé pour créer la connexion.
> Si l'application est installée dans un espace de travail Bitbucket, vous avez besoin des autorisations Gérer l'espace de travail. Dans le cas contraire, l'option d'installation de l'application ne s'affichera pas.

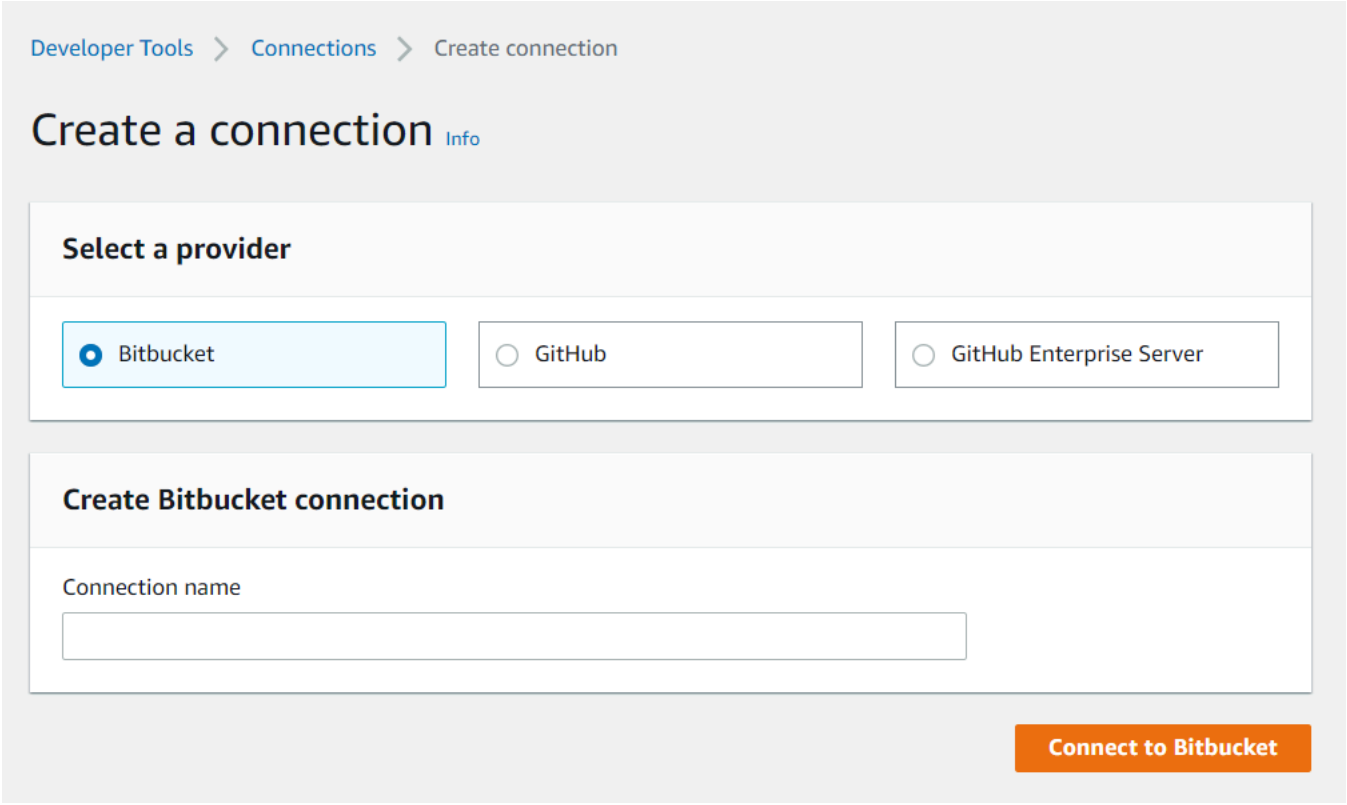
Rubriques

Créer une connexion à Bitbucket (console)

Étape 1 : Créer votre connexion

1. Connectez-vous à la AWS Management Console console AWS Developer Tools et ouvrez-la à l'adressehttps://console.aws.amazon.com/codesuite/settings/connections.
2. Choisissez Settings > Connections (Paramètres > Connexions), puis Create connection (Créer une connexion).

3. Pour créer une connexion à un référentiel Bitbucket, sous Select a provider (Sélectionner un fournisseur), choisissez Bitbucket. Dans Connection name (Nom de la connexion), saisissez le nom de la connexion que vous souhaitez créer. Choisissez Connect to Bitbucket (Se connecter à Bitbucket), puis passez à l'étape 2.

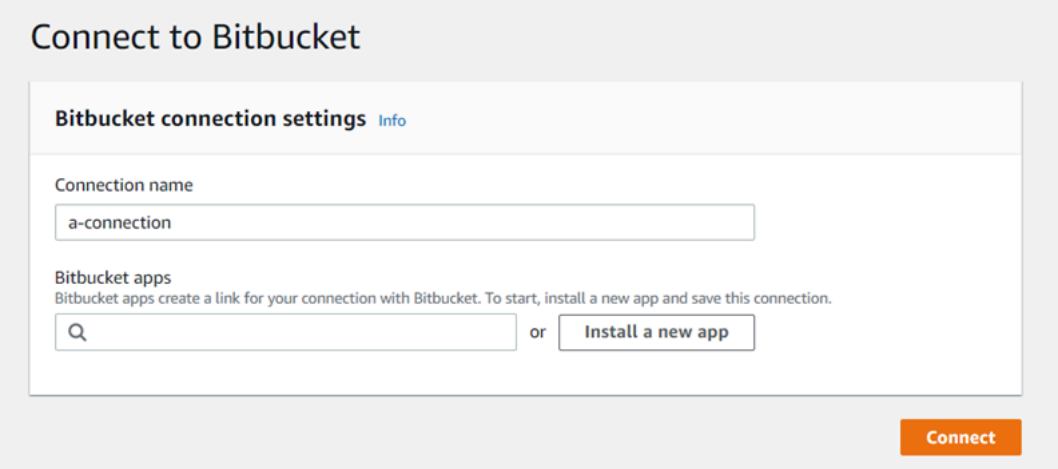


Étape 2 : Se connecter à Bitbucket

1. Dans la page des paramètres Connect to Bitbucket (Se connecter à Bitbucket), votre nom de connexion s'affiche.

   Sous Bitbucket apps (Applications Bitbucket), choisissez une installation d'application ou choisissez Install a new app (Installer une nouvelle application) pour en créer une.

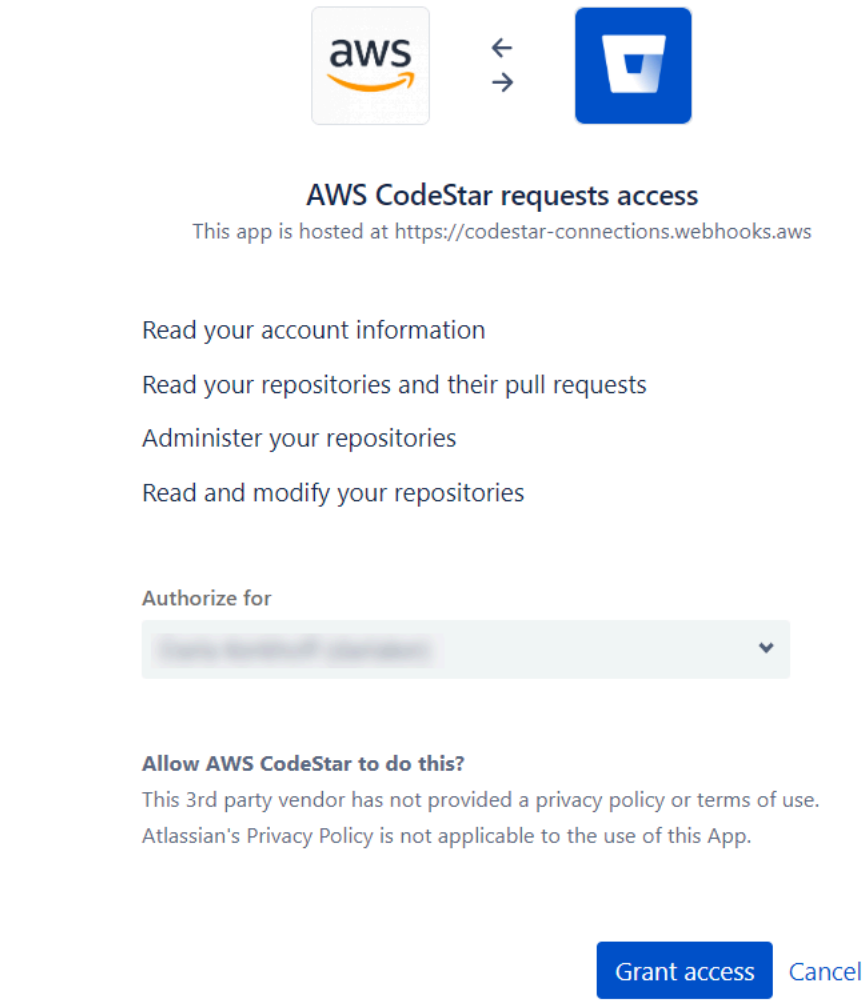
> **Note**
>
> Vous n'installez l'application qu'une seule fois pour chaque espace de travail ou compte Bitbucket. Si vous avez déjà installé l'application Bitbucket, sélectionnez-la et passez à la dernière étape de cette section.



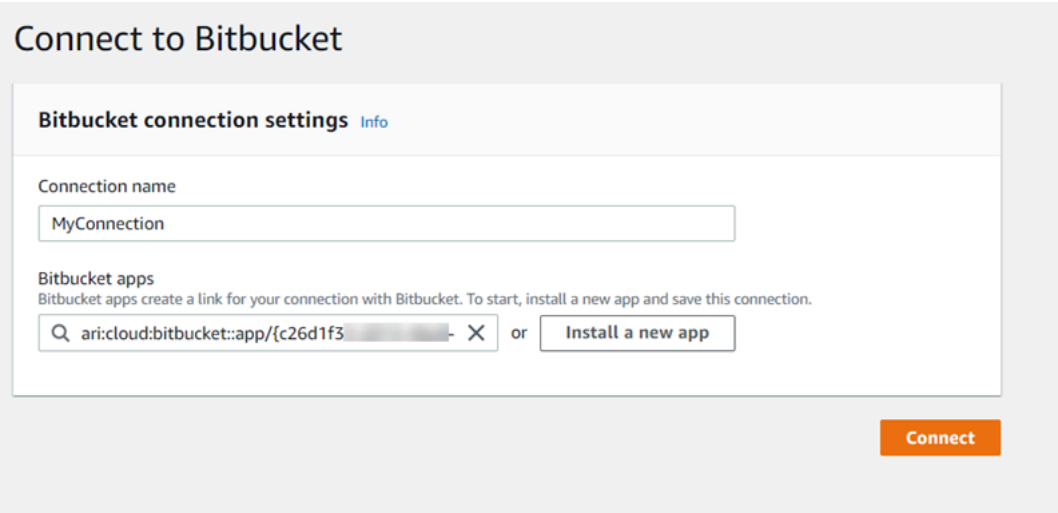
2. Si la page de connexion pour Bitbucket s'affiche, connectez-vous avec vos informations d'identification, puis choisissez de continuer.
3. Sur la page d'installation de l'application, un message indique que l' AWS CodeStar application essaie de se connecter à votre compte Bitbucket.

   Si vous utilisez un espace de travail Bitbucket, modifiez l'option Autoriser pour pour l'espace de travail. Seuls les espaces de travail auxquels vous avez accès en tant qu'administrateur s'affichent.

   Choisissez Grant access (Accorder l'accès).



4. Dans Bitbucket apps (Applications Bitbucket), l'ID de connexion de votre nouvelle installation s'affiche. Choisissez Se connecter. La connexion créée s'affiche dans la liste des connexions.



Créer une connexion à Bitbucket (CLI)

Vous pouvez utiliser le AWS Command Line Interface (AWS CLI) pour créer une connexion.

Pour ce faire, utilisez la commande create-connection.

> **Important**
>
> Une connexion créée via le AWS CLI ou AWS CloudFormation est en `PENDING` état par défaut. Après avoir créé une connexion à l'aide de la CLI AWS CloudFormation, utilisez la console pour modifier la connexion afin de définir son état`AVAILABLE`.

Pour créer une connexion à Bitbucket

1. Ouvrez une invite de terminal (Linux, macOS ou Unix) ou de commande (Windows). Utilisez le AWS CLI pour exécuter la create-connection commande, en spécifiant le `--provider-type` et `--connection-name` pour votre connexion. Dans cet exemple, le nom du fournisseur tiers est `Bitbucket` et le nom de connexion spécifié est `MyConnection`.

   ```
   aws codestar-connections create-connection --provider-type Bitbucket --connection-
   name MyConnection
   ```

   En cas de succès, cette commande renvoie les informations ARN de connexion semblables à ce qui suit.

   ```
   {
       "ConnectionArn": "arn:aws:codestar-connections:us-west-2:account_id:connection/
   aEXAMPLE-8aad-4d5d-8878-dfcab0bc441f"
   }
   ```

2. Utilisez la console pour terminer la connexion. Pour plus d'informations, consultez Mettre à jour une connexion en attente.

Créez une connexion avec GitHub

Vous pouvez utiliser le AWS Management Console ou le AWS Command Line Interface (AWS CLI) pour créer une connexion à GitHub.

Avant de commencer :

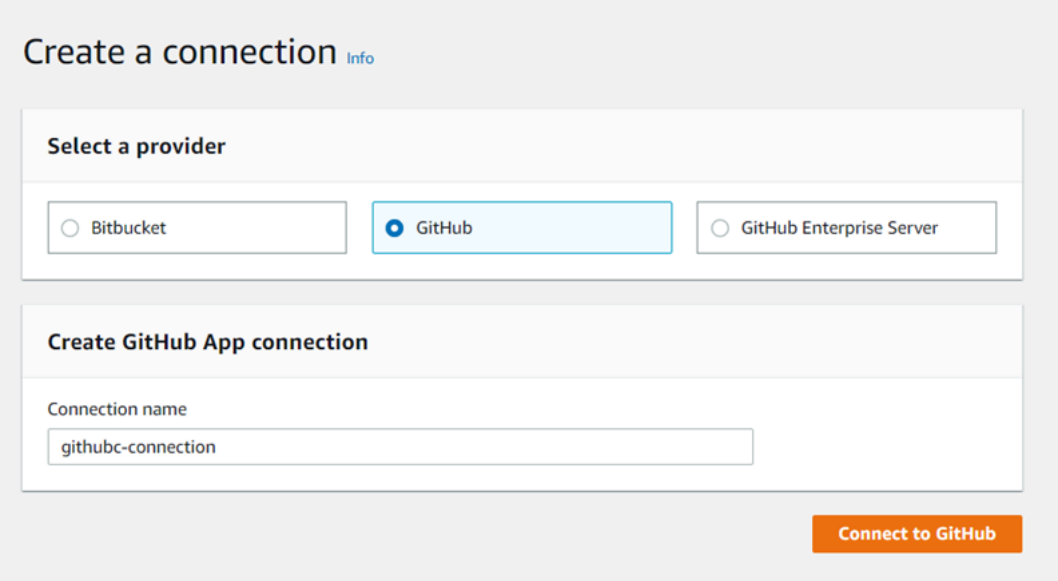
- Vous devez déjà avoir créé un compte auprès de GitHub.
- Vous devez déjà avoir créé votre référentiel de code tiers.

> **Note**
>
> Pour créer la connexion, vous devez être le propriétaire de GitHub l'organisation. Pour les référentiels qui ne font pas partie d'une organisation, vous devez être le propriétaire du référentiel.

Rubriques

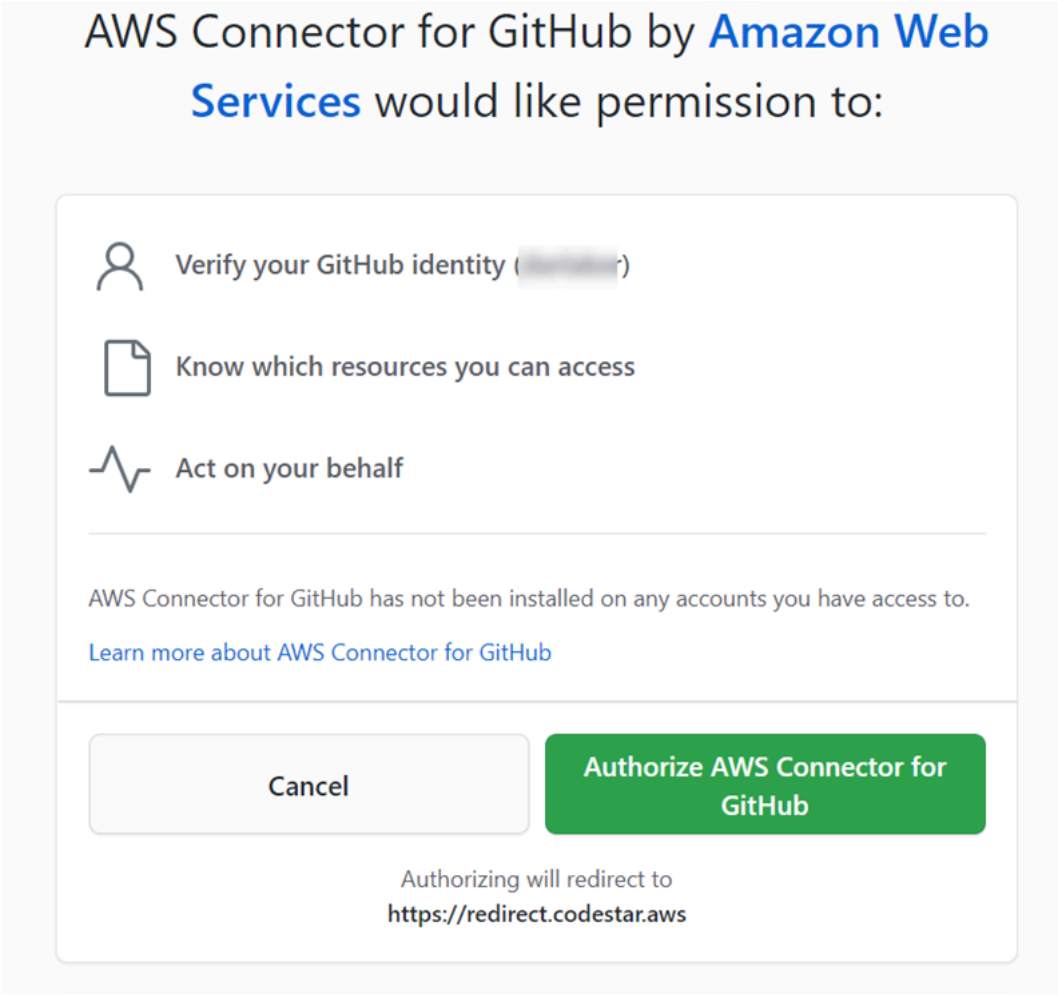
Création d'une connexion à GitHub (console)

1. Connectez-vous à la AWS Management Console console Developer Tools et ouvrez-la à l'adressehttps://console.aws.amazon.com/codesuite/settings/connections.
2. Choisissez Settings > Connections (Paramètres > Connexions), puis Create connection (Créer une connexion).
3. Pour créer une connexion à un référentiel GitHub ou à un référentiel GitHub Enterprise Cloud, sous Sélectionnez un fournisseur, choisissez GitHub. Dans Connection name (Nom de la connexion), saisissez le nom de la connexion que vous souhaitez créer. Choisissez Connect to GitHub, puis passez à l'étape 2.

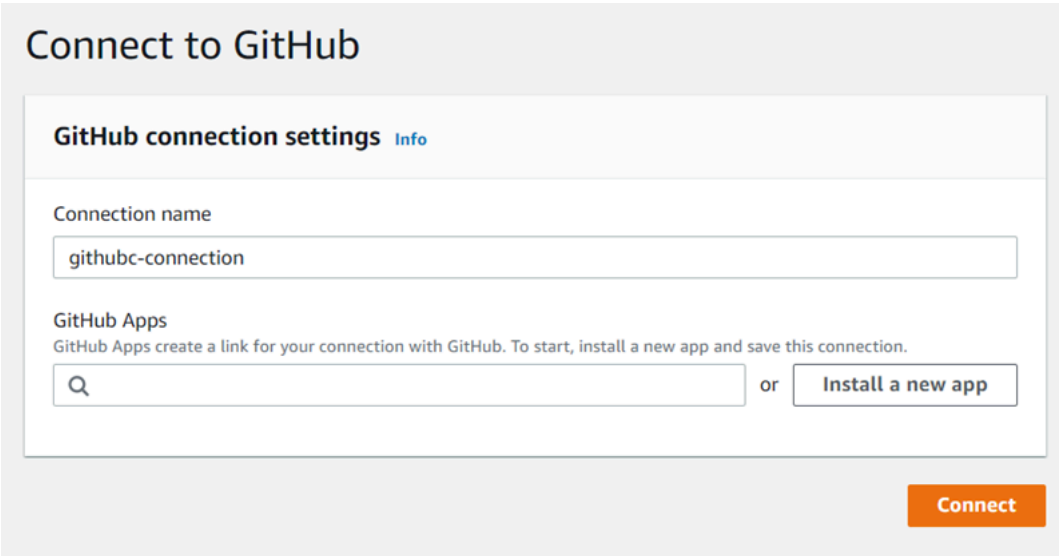


Pour créer une connexion avec GitHub

1. Dans les paramètres de GitHub connexion, le nom de votre connexion apparaît dans Nom de la connexion. Choisissez Connect to (Se connecter à) GitHub. La page de demande d'accès s'affiche.



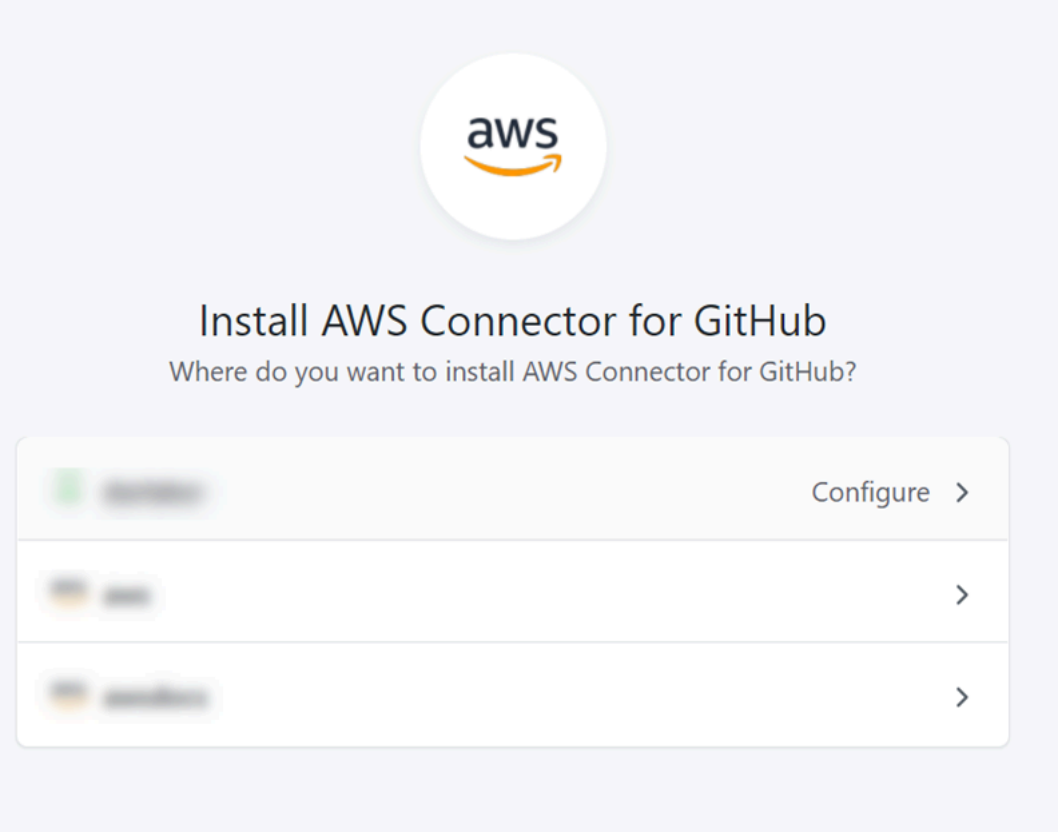
2. Choisissez Autoriser le AWS connecteur pour GitHub. La page de connexion affiche et affiche le champ GitHub Applications.



3. Sous GitHub Applications, choisissez une installation d'application ou choisissez Installer une nouvelle application pour en créer une.

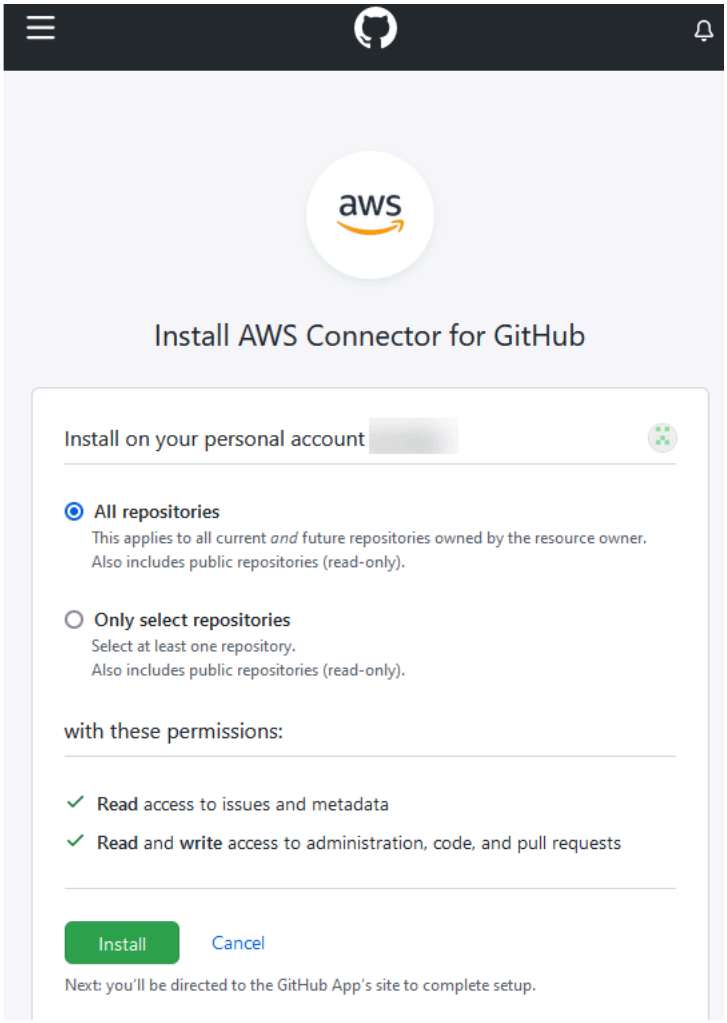
> **Note**
>
> Installez une application pour toutes vos connexions à un fournisseur particulier. Si vous avez déjà installé le AWS Connector for GitHub app, choisissez-le et ignorez cette étape.

4. Sur la GitHub page Installer le AWS connecteur pour, choisissez le compte sur lequel vous souhaitez installer l'application.



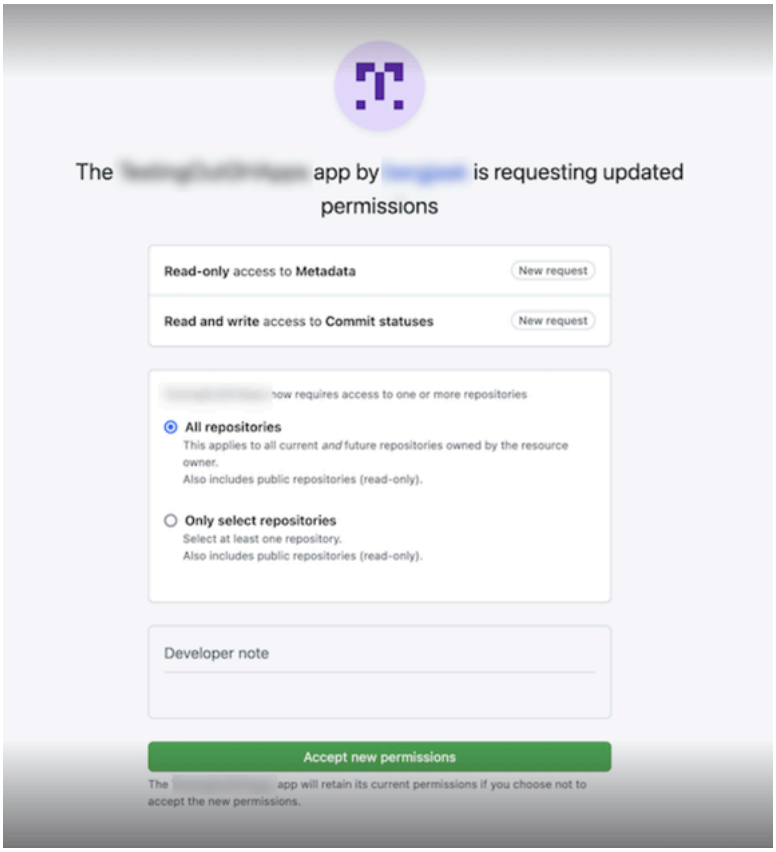
> **Note**
>
> Vous n'installez l'application qu'une seule fois pour chaque GitHub compte. Si vous avez déjà installé l'application, vous pouvez choisir Configure (Configurer) pour passer à une page de modification pour l'installation de votre application, ou vous pouvez utiliser le bouton Précédent pour revenir à la console.

5. Sur la GitHub page Installer le AWS connecteur pour, laissez les valeurs par défaut et choisissez Installer.



Après cette étape, une page d'autorisations mise à jour peut s'afficher GitHub.

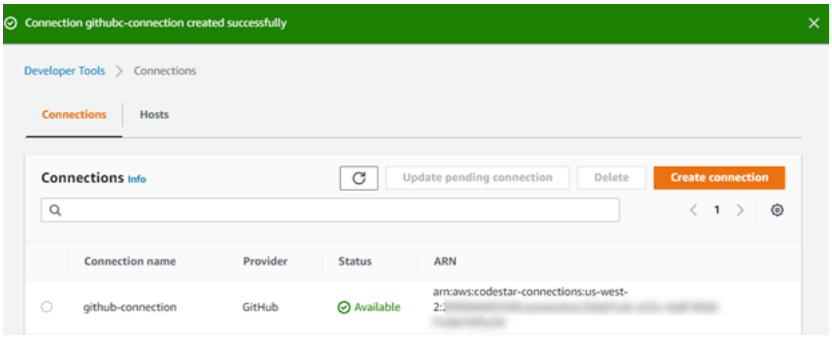
6. Si une page s'affiche indiquant que des autorisations ont été mises à jour pour le AWS Connector pour GitHub l'application, choisissez Accepter les nouvelles autorisations.



7. Vous revenez à la GitHub page Connect to. L'identifiant de connexion de votre nouvelle installation apparaît dans GitHubApps. Choisissez Connect (Connexion).

Consultez votre connexion créée

- La connexion créée s'affiche dans la liste des connexions.



Création d'une connexion à GitHub (CLI)

Vous pouvez utiliser le AWS Command Line Interface (AWS CLI) pour créer une connexion à GitHub.

Pour ce faire, utilisez la commande create-connection.

> **Important**
>
> Une connexion créée via le AWS CLI ou AWS CloudFormation est en `PENDING` état par défaut. Après avoir créé une connexion à l'aide de la CLI AWS CloudFormation, utilisez la console pour modifier la connexion afin de définir son état`AVAILABLE`.

Pour créer une connexion avec GitHub

1. Ouvrez une invite de terminal (Linux, macOS ou Unix) ou de commande (Windows). Utilisez le AWS CLI pour exécuter la create-connection commande, en spécifiant le `--provider-type` et `--connection-name` pour votre connexion. Dans cet exemple, le nom du fournisseur tiers est `GitHub` et le nom de connexion spécifié est `MyConnection`.

   ```
   aws codestar-connections create-connection --provider-type GitHub --connection-name
    MyConnection
   ```

   En cas de succès, cette commande renvoie les informations ARN de connexion semblables à ce qui suit.

   ```
   {
       "ConnectionArn": "arn:aws:codestar-connections:us-west-2:account_id:connection/
   aEXAMPLE-8aad-4d5d-8878-dfcab0bc441f"
   }
   ```

2. Utilisez la console pour terminer la connexion. Pour plus d'informations, consultez Mettre à jour une connexion en attente.

Création d'une connexion à GitHub Enterprise Server

Vous utilisez des connexions pour associer vos AWS ressources à un référentiel tiers. Vous pouvez utiliser le AWS Management Console ou le AWS Command Line Interface (AWS CLI) pour créer une connexion à GitHub Enterprise Server.

Les connexions fournissent uniquement l'accès aux référentiels détenus par le compte GitHub Enterprise Server qui est utilisé lors de la création de la connexion pour autoriser l'installation de l' GitHubapplication.

Avant de commencer :

- Vous devez déjà disposer d'une instance GitHub d'Enterprise Server et d'un référentiel.
- Vous devez être administrateur de l'instance GitHub Enterprise Server pour créer des GitHub applications et créer une ressource hôte, comme indiqué dans cette section.

> **Important**
>
> Lorsque vous configurez votre hôte pour GitHub Enterprise Server, un point de terminaison VPC pour les données d'événements des webhooks est créé pour vous. Si vous avez créé votre hôte avant le 24 novembre 2020 et que vous souhaitez utiliser des points de terminaison PrivateLink Webhook VPC, vous devez d'abord supprimer votre hôte, puis en créer un nouveau.

Rubriques

- Création d'une connexion à GitHub Enterprise Server (console)
- Création d'une connexion à GitHub Enterprise Server (CLI)

Création d'une connexion à GitHub Enterprise Server (console)

Pour créer une connexion GitHub Enterprise Server, vous devez fournir des informations sur l'emplacement d'installation de votre GitHub Enterprise Server et autoriser la création de la connexion à l'aide de vos informations d'identification GitHub Enterprise.

Rubriques

- Créez votre connexion au serveur GitHub d'entreprise (console)

Créez votre connexion au serveur GitHub d'entreprise (console)

Pour créer une connexion à GitHub Enterprise Server, munissez-vous de l'URL de votre serveur et de vos informations d'identification GitHub Enterprise.

Pour créer un hôte

1. Connectez-vous à la AWS Management Console console AWS Developer Tools et ouvrez-la à l'adressehttps://console.aws.amazon.com/codesuite/settings/connections.

2. Sur l'ongle Hosts (Hôtes), choisissez Create host (Créer un hôte).
3. Dans Host name (Nom d'hôte), saisissez le nom que vous souhaitez utiliser pour votre hôte.
4. Dans Sélectionner un fournisseur, choisissez l'une des options suivantes :

   - GitHub Serveur d'entreprise
   - GitLab autogéré

5. Dans URL, saisissez le point de terminaison de l'infrastructure sur laquelle votre fournisseur est installé.
6. Si votre serveur est configuré dans un VPC Amazon et que vous souhaitez vous connecter à votre VPC, choisissez Use a VPC (Utiliser un VPC). Sinon, choisissez No VPC.
7. Si vous avez lancé votre instance dans un VPC Amazon et que vous souhaitez vous connecter à votre VPC, choisissez Use a VPC (Utiliser un VPC) et complétez ce qui suit.

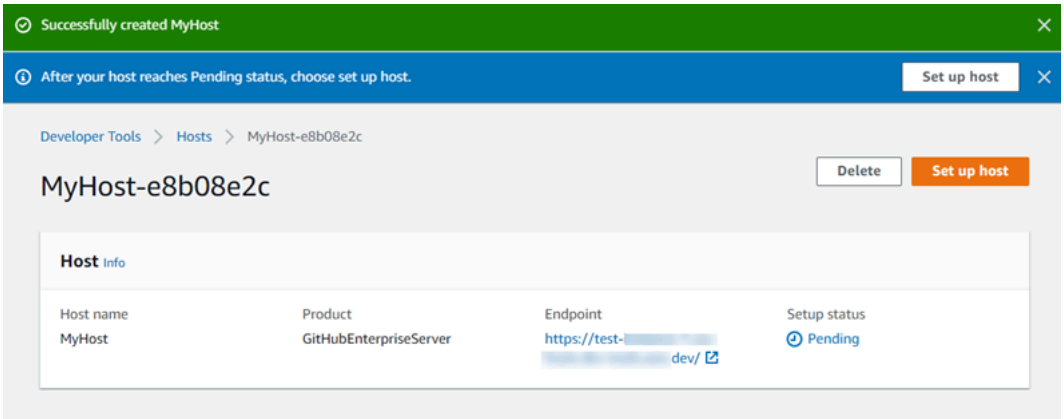
   a. Dans ID du VPC, choisissez votre ID de VPC. Veillez à choisir le VPC de l'infrastructure sur laquelle votre instance est installée ou un VPC qui a accès à votre instance via VPN ou Direct Connect.

   b. Si vous avez configuré un VPC privé et que vous avez configuré votre instance pour effectuer la validation TLS à l'aide d'une autorité de certification non publique, dans Certificat TLS, saisissez votre ID de certificat. La valeur du certificat TLS est la clé publique du certificat.

8. Choisissez Create host (Créer un hôte).
9. Une fois la page des détails de l'hôte affichée, l'état de l'hôte change au fur et à mesure que l'hôte est créé.

> **Note**
>
> Si la configuration de votre hôte inclut une configuration VPC, prévoyez plusieurs minutes pour l'approvisionnement des composants du réseau hôte.

Attendez que votre hôte atteigne l'état En attente, puis terminez la configuration. Pour plus d'informations, consultez Configurer un hôte en attente.

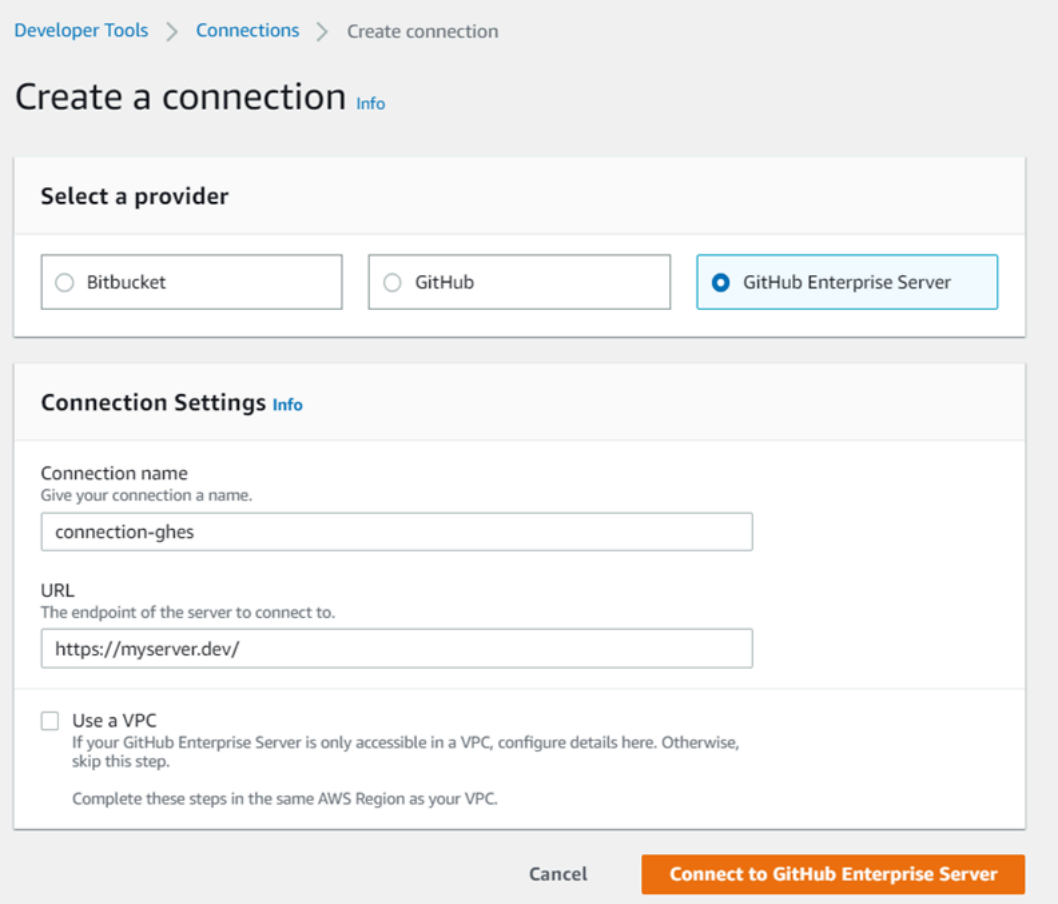


Étape 2 : créer votre connexion à GitHub Enterprise Server (console)

1. Connectez-vous à la console Developer Tools AWS Management Console et ouvrez-la à l'adressehttps://console.aws.amazon.com/codesuite/settings/connections.
2. Choisissez Settings > Connections (Paramètres > Connexions), puis Create connection (Créer une connexion).
3. Pour créer une connexion à un référentiel GitHub Enterprise Server installé, choisissez GitHub Enterprise Server.

Se connecter au serveur GitHub d'entreprise

1. Dans Connection name (Nom de la connexion), saisissez le nom de votre connexion.



2. Dans URL, saisissez le point de terminaison de votre serveur.

> **Note**
>
> Si l'URL fournie a déjà été utilisée pour configurer un serveur d' GitHubentreprise pour une connexion, vous serez invité à choisir l'ARN de la ressource hôte créé précédemment pour ce point de terminaison.

3. (Facultatif) Si vous avez lancé votre serveur dans un VPC Amazon et que vous souhaitez vous connecter avec votre VPC, choisissez Utiliser un VPC et procédez comme suit.

   a. Dans ID du VPC, choisissez votre ID de VPC. Assurez-vous de choisir le VPC pour l'infrastructure sur laquelle votre instance de serveur GitHub d'entreprise est installée ou un VPC avec accès à votre instance de serveur GitHub d'entreprise via VPN ou Direct Connect.

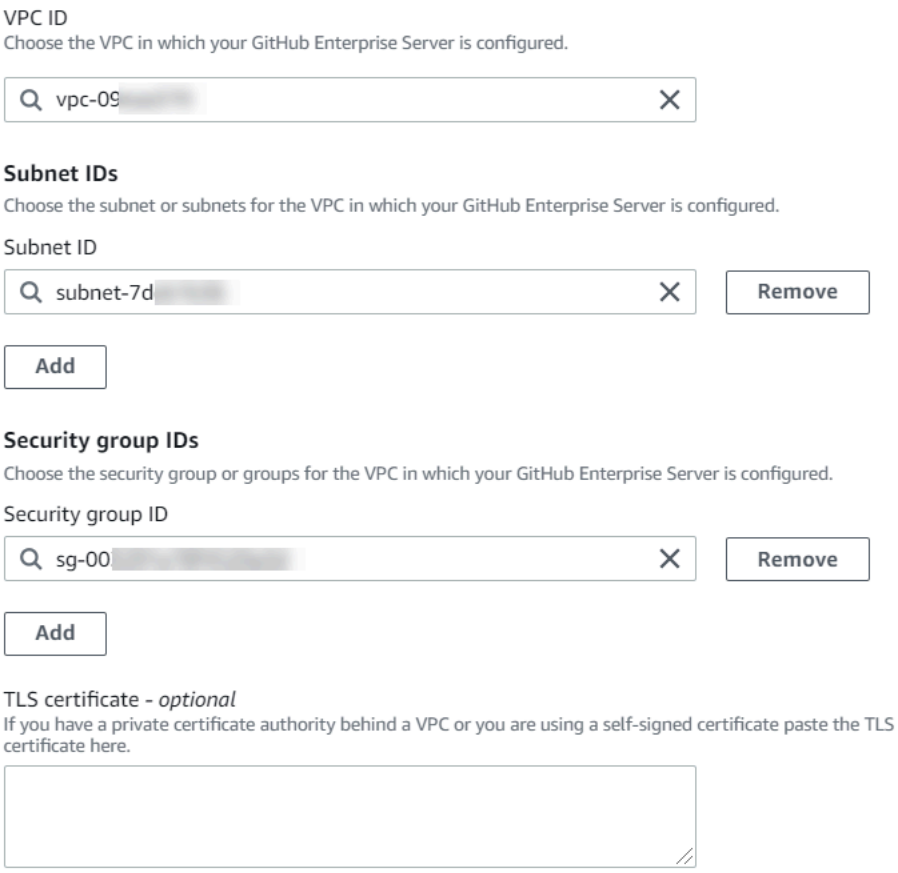
   b. Sous Subnet ID (ID de sous-réseau), choisissez Add (Ajouter). Dans le champ, choisissez l'ID de sous-réseau que vous souhaitez utiliser pour votre hôte. Vous pouvez choisir jusqu'à 10 sous-réseaux.

Assurez-vous de choisir le sous-réseau pour l'infrastructure dans laquelle votre instance de serveur GitHub d'entreprise est installée ou un sous-réseau avec accès à votre instance de serveur GitHub d'entreprise installée via VPN ou Direct Connect.

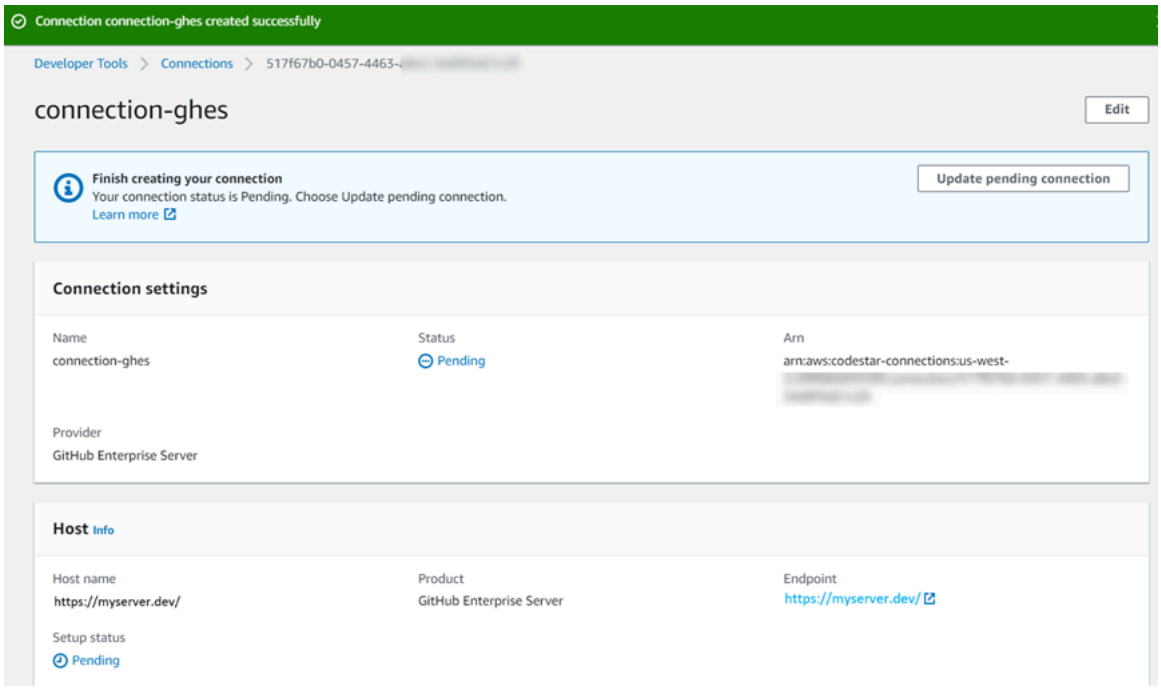
c. Sous Security group IDs (ID de groupe de sécurité), choisissez Add (Ajouter). Dans le champ, choisissez le groupe de sécurité que vous souhaitez utiliser pour votre hôte. Vous pouvez choisir jusqu'à 10 groupes de sécurité.

   Assurez-vous de choisir le groupe de sécurité pour l'infrastructure sur laquelle votre instance de serveur GitHub d'entreprise est installée ou un groupe de sécurité ayant accès à votre instance de serveur GitHub d'entreprise installée via un VPN ou Direct Connect.

d. Si vous avez configuré un VPC privé et que vous avez configuré votre instance de serveur GitHub d'entreprise pour effectuer une validation TLS à l'aide d'une autorité de certification non publique, dans Certificat TLS, entrez votre ID de certificat. La valeur du certificat TLS doit être la clé publique du certificat.

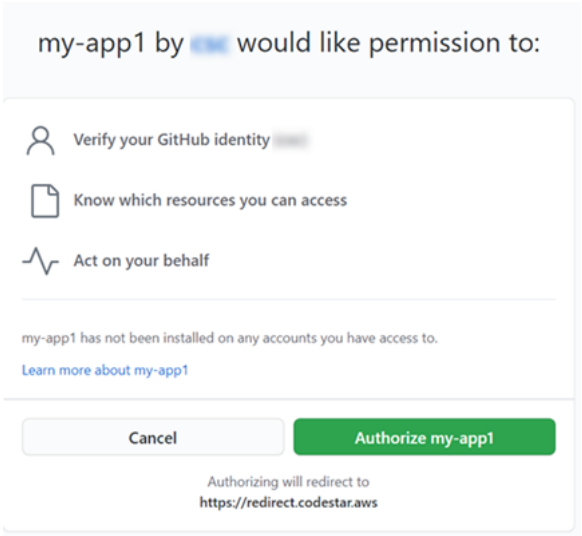


4. Choisissez Connect to GitHub Enterprise Server. La connexion créée s'affiche avec le statut En attente. Une ressource hôte est créée pour la connexion avec les informations de serveur que vous avez fournies. Pour le nom d'hôte, l'URL est utilisée.
5. Choisissez Update pending connection (Mettre à jour la connexion en attente).



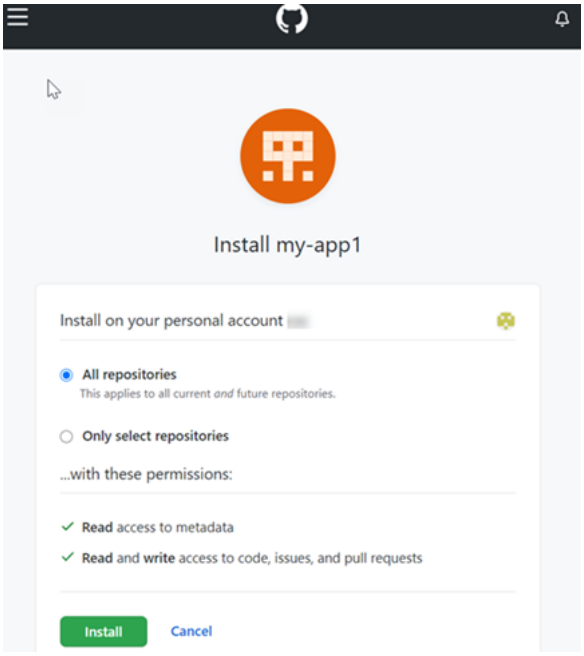
6. Si vous y êtes invité, sur la page de connexion GitHub Enterprise, connectez-vous avec vos informations GitHub d'identification Enterprise.
7. Sur la page Créer une GitHub application, choisissez un nom pour votre application.

8. Sur la page GitHub d'autorisation, choisissez Autoriser<app-name>.



9. Sur la page d'installation de l'application, un message indique que l'application AWS CodeStar Connector est prête à être installée. Si vous avez plusieurs organisations, vous pouvez être invité à choisir l'organisation dans laquelle vous souhaitez installer l'application.

   Choisissez les paramètres du référentiel dans lesquels vous souhaitez installer l'application. Choisissez Installer.



10. La page de connexion affiche la connexion créée avec un statut Disponible.

Création d'une connexion à GitHub Enterprise Server (CLI)

Vous pouvez utiliser le AWS Command Line Interface (AWS CLI) pour créer une connexion.

Pour ce faire, utilisez les commandes create-host et create-connection.

> **Important**
>
> Une connexion créée via le AWS CLI ou AWS CloudFormation est en `PENDING` état par défaut. Après avoir créé une connexion à l'aide de la CLI AWS CloudFormation, utilisez la console pour modifier la connexion afin de définir son état`AVAILABLE`.

Étape 1 : Pour créer un hôte pour GitHub Enterprise Server (CLI)

1. Ouvrez une invite de terminal (Linux, macOS ou Unix) ou de commande (Windows). Utilisez le AWS CLI pour exécuter la create-host commande, en spécifiant le `--name``--provider-type`, et `--provider-endpoint` pour votre connexion. Dans cet exemple, le nom du fournisseur tiers est `GitHubEnterpriseServer` et le point de terminaison est `my-instance.dev`.

   ```
   aws codestar-connections create-host --name MyHost --provider-type
    GitHubEnterpriseServer --provider-endpoint "https://my-instance.dev"
   ```

En cas de succès, cette commande renvoie les informations Amazon Resource Name (ARN) hôte semblables à ce qui suit.

```
{
    "HostArn": "arn:aws:codestar-connections:us-west-2:account_id:host/My-
Host-28aef605"
}
```

Après cette étape, l'hôte présente l'état `PENDING`.

2. Utilisez la console pour terminer la configuration de l'hôte et passer l'hôte vers l'état `Available`. Pour plus d'informations, consultez Configurer un hôte en attente.

Étape 2 : Configurer un hôte en attente dans la console

1. Connectez-vous à la console Developer Tools AWS Management Console et ouvrez-la à l'adressehttps://console.aws.amazon.com/codesuite/settings/connections.
2. Utilisez la console pour terminer la configuration de l'hôte et passer l'hôte vers l'état `Available`. veuillez consulter Configurer un hôte en attente.

Étape 3 : Pour créer une connexion pour GitHub Enterprise Server (CLI)

1. Ouvrez une invite de terminal (Linux, macOS ou Unix) ou de commande (Windows). Utilisez le AWS CLI pour exécuter la create-connection commande, en spécifiant le `--host-arn` et `--connection-name` pour votre connexion.

```
aws codestar-connections create-connection --host-arn arn:aws:codestar-
connections:us-west-2:account_id:host/MyHost-234EXAMPLE --connection-name
 MyConnection
```

En cas de succès, cette commande renvoie les informations ARN de connexion semblables à ce qui suit.

```
{
    "ConnectionArn": "arn:aws:codestar-connections:us-west-2:account_id:connection/
aEXAMPLE-8aad"
}
```

2. Utilisez la console pour configurer la connexion en attente. Pour plus d'informations, consultez Mettre à jour une connexion en attente.

Étape 4 : Pour établir une connexion pour GitHub Enterprise Server dans la console

1. Connectez-vous à la console Developer Tools AWS Management Console et ouvrez-la à l'adressehttps://console.aws.amazon.com/codesuite/settings/connections.
2. Utilisez la console pour configurer la connexion en attente et la faire passer à l'état `Available`. Pour plus d'informations, consultez Mettre à jour une connexion en attente.

Créez une connexion avec GitLab

Vous pouvez utiliser le AWS Management Console ou le AWS Command Line Interface (AWS CLI) pour créer une connexion à un dépôt hébergé sur gitlab.com.

> **Note**
>
> En autorisant l'installation de cette connexion GitLab, vous autorisez notre service à traiter vos données, et vous pouvez révoquer ces autorisations à tout moment en désinstallant l'application.

Avant de commencer :

- Vous devez déjà avoir créé un compte auprès de GitLab.

> **Note**
>
> Les connexions fournissent uniquement l'accès au compte qui a été utilisé pour créer et autoriser la connexion.

> **Note**
>
> Vous pouvez créer des connexions dans lesquelles vous avez le rôle de propriétaire GitLab, puis la connexion peut être utilisée avec le référentiel avec des ressources telles

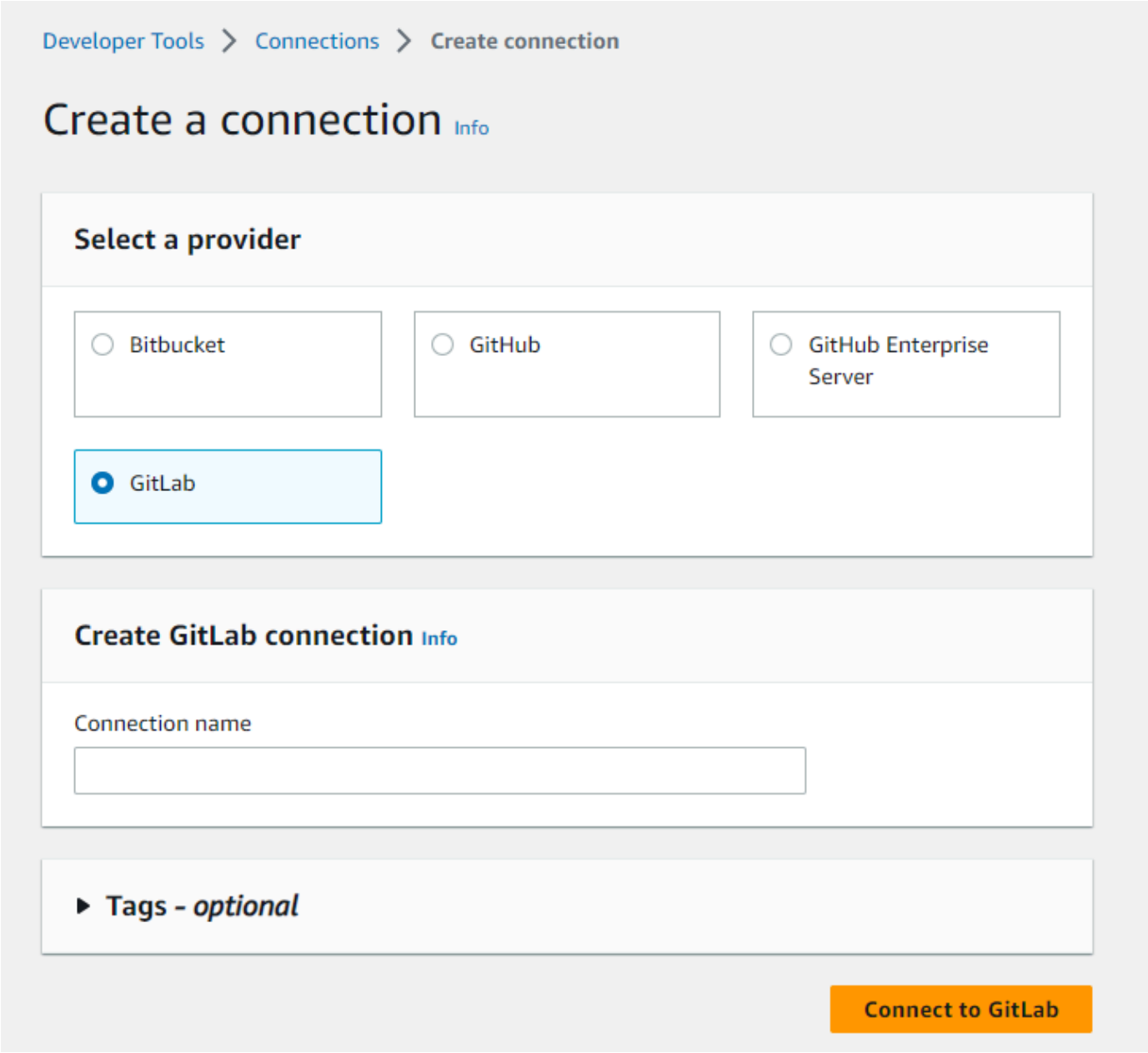
que CodePipeline. Pour les référentiels dans des groupes, il n'est pas nécessaire d'être le propriétaire du groupe.

Rubriques

Création d'une connexion à GitLab (console)

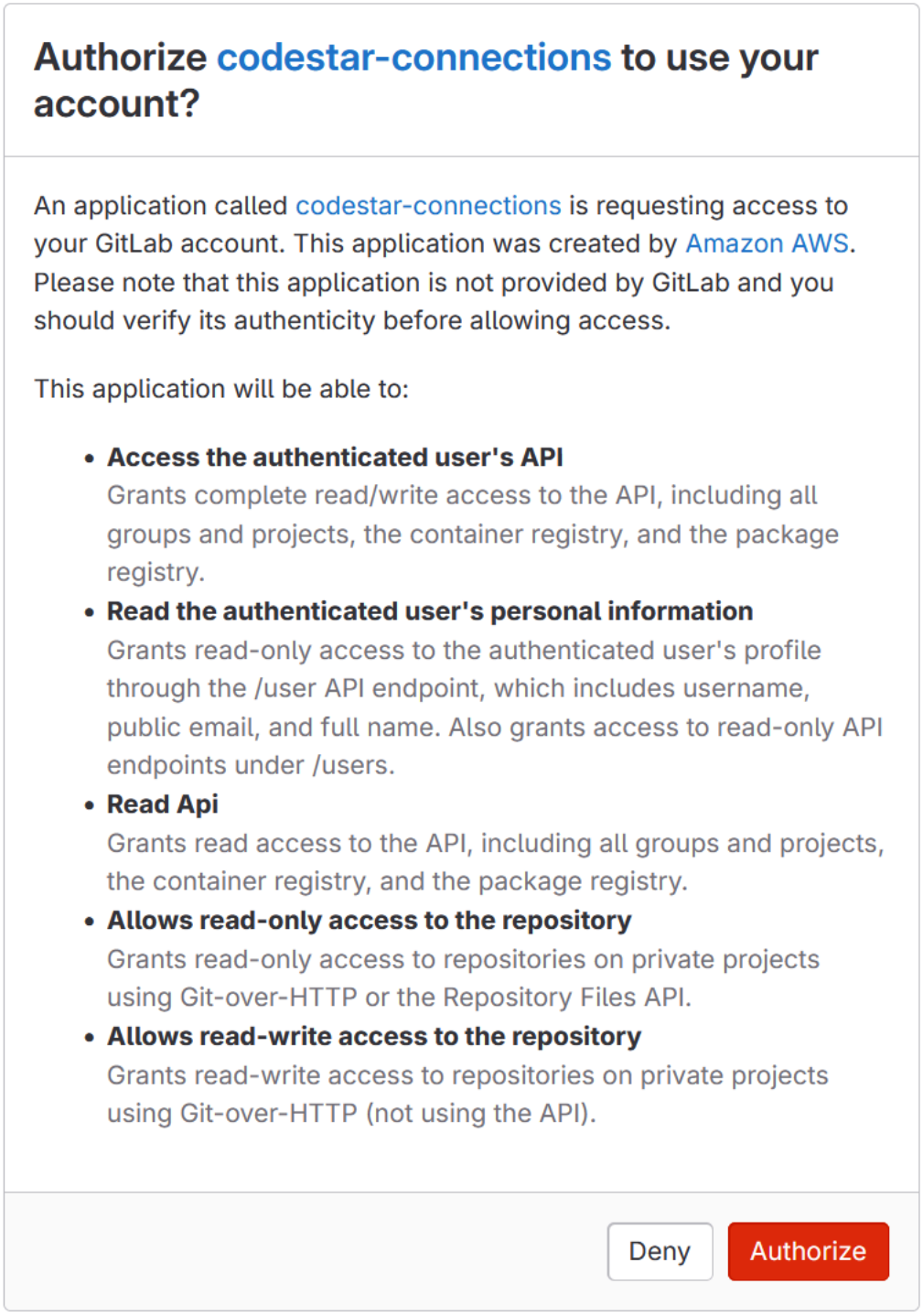
Étape 1 : Créer votre connexion

1. Connectez-vous à AWS Management Console, puis ouvrez la console AWS Developer Tools à l'adressehttps://console.aws.amazon.com/codesuite/settings/connections.
2. Choisissez Paramètres, puis choisissez Connexions. Choisissez Créer une connexion.
3. Pour créer une connexion à un GitLab référentiel, sous Sélectionnez un fournisseur, sélectionnez GitLab. Dans Connection name (Nom de la connexion), saisissez le nom de la connexion que vous souhaitez créer. Choisissez Connect to GitLab.



4. Lorsque la page de connexion GitLab s'affiche, connectez-vous avec vos informations d'identification, puis choisissez Se connecter.
5. Une page d'autorisation s'affiche avec un message demandant l'autorisation de connexion pour accéder à votre GitLab compte.

   Choisissez Authorize (Autoriser).



6. Le navigateur revient à la page de la console des connexions. Sous Créer une GitLab connexion, la nouvelle connexion est affichée dans Nom de la connexion.
7. Choisissez Connect to GitLab.

Une fois la connexion créée avec succès, une bannière de réussite s'affiche. Les détails de la connexion sont affichés sur la page Paramètres de connexion.

Création d'une connexion à GitLab (CLI)

Vous pouvez utiliser le AWS Command Line Interface (AWS CLI) pour créer une connexion.

Pour ce faire, utilisez la commande create-connection.

> **Important**
>
> Une connexion créée via le AWS CLI ou AWS CloudFormation est en `PENDING` état par défaut. Après avoir créé une connexion à l'aide de la CLI AWS CloudFormation, utilisez la console pour modifier la connexion afin de définir son état`AVAILABLE`.

Pour créer une connexion avec GitLab

1. Ouvrez une invite de terminal (Linux, macOS ou Unix) ou de commande (Windows). Utilisez le AWS CLI pour exécuter la create-connection commande, en spécifiant le `--provider-type` et `--connection-name` pour votre connexion. Dans cet exemple, le nom du fournisseur tiers est `GitLab` et le nom de connexion spécifié est `MyConnection`.

   ```
   aws codestar-connections create-connection --provider-type GitLab --connection-name
    MyConnection
   ```

   En cas de succès, cette commande renvoie les informations ARN de connexion semblables à ce qui suit.

   ```
   {
       "ConnectionArn": "arn:aws:codestar-connections:us-west-2:account_id:connection/
   aEXAMPLE-8aad-4d5d-8878-dfcab0bc441f"
   }
   ```

2. Utilisez la console pour terminer la connexion. Pour plus d'informations, consultez Mettre à jour une connexion en attente.

Création d'une connexion à l' GitLabautogestion

Vous pouvez créer des connexions pour GitLab Enterprise Edition ou GitLab Community Edition avec une installation autogérée.

Vous pouvez utiliser le AWS Management Console ou le AWS Command Line Interface (AWS CLI) pour créer une connexion et un hôte à des fins d' GitLab autogestion.

> **Note**
>
> En autorisant cette application de connexion en mode GitLab autogérée, vous autorisez notre service à traiter vos données, et vous pouvez révoquer ces autorisations à tout moment en désinstallant l'application.

Avant de créer une connexion à GitLab Automanaged, vous devez créer un hôte à utiliser pour la connexion, comme indiqué dans ces étapes. Pour voir une présentation du flux de travail de création d'hôte pour les fournisseurs installés, consultez Flux de travail de création ou de mise à jour d'un hôte.

Vous pouvez éventuellement configurer votre hôte avec un VPC. Pour plus d'informations sur la configuration réseau et de VPC pour votre ressource hôte, consultez les prérequis pour les VPC dans (Facultatif) Prérequis : configuration réseau ou d'Amazon VPC pour votre connexion et Résolution des problèmes liés à la configuration d'un VPC pour votre hôte.

Avant de commencer :

- Vous devez déjà avoir créé un compte GitLab et disposer de l'édition GitLab Enterprise ou de l'édition GitLab Community avec une installation autogérée. Pour plus d'informations, consultez https://docs.gitlab.com/ee/subscriptions/self_managed/.

  > **Note**
  >
  > Les connexions fournissent uniquement l'accès au compte qui a été utilisé pour créer et autoriser la connexion.

> **Note**
>
> Vous pouvez créer des connexions à un référentiel dans lequel vous avez le rôle de propriétaire GitLab, puis la connexion peut être utilisée avec des ressources telles que CodePipeline. Pour les référentiels dans des groupes, il n'est pas nécessaire d'être le propriétaire du groupe.

- Vous devez déjà avoir créé un jeton d'accès GitLab personnel (PAT) avec l'autorisation limitée suivante uniquement : api. Pour plus d'informations, consultez https://docs.gitlab.com/ee/user/profile/personal_access_tokens.html. Seul le PAT utilisé par un administrateur peut être utilisé.

> **Note**
>
> Votre PAT est utilisé pour autoriser l'hôte et n'est pas stocké ni utilisé par les connexions à d'autres fins. Pour configurer un hôte, vous pouvez créer un PAT temporaire, puis, une fois l'hôte configuré, vous pouvez le supprimer.

Rubriques

Création d'une connexion à l' GitLab autogestion (console)

Suivez ces étapes pour créer un hôte et une connexion GitLab autogérés dans la console. Pour voir les considérations relatives à la configuration d'un hôte dans un VPC, consultez (Facultatif) Prérequis : configuration réseau ou d'Amazon VPC pour votre connexion.

> **Note**
>
> Vous créez un hôte pour une seule installation GitLab autogérée, puis vous pouvez gérer une ou plusieurs connexions GitLab autogérées avec cet hôte.

Étape 1 : Créer votre hôte

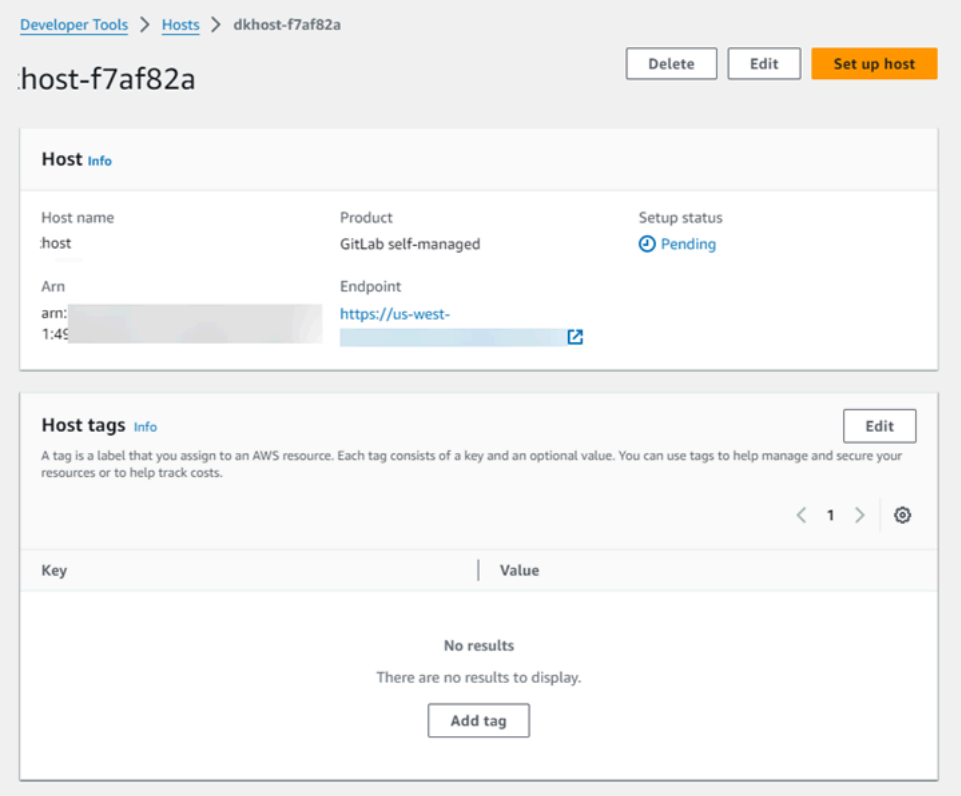
1. Connectez-vous à AWS Management Console, puis ouvrez la console AWS Developer Tools à l'adressehttps://console.aws.amazon.com/codesuite/settings/connections.
2. Sur l'ongle Hosts (Hôtes), choisissez Create host (Créer un hôte).
3. Dans Host name (Nom d'hôte), saisissez le nom que vous souhaitez utiliser pour votre hôte.
4. Dans Sélectionnez un fournisseur, sélectionnez GitLabAutogéré.
5. Dans URL, saisissez le point de terminaison de l'infrastructure sur laquelle votre fournisseur est installé.
6. Si votre serveur est configuré dans un VPC Amazon et que vous souhaitez vous connecter à votre VPC, choisissez Use a VPC (Utiliser un VPC). Sinon, choisissez No VPC.
7. (Facultatif) Si vous avez lancé votre hôte dans un VPC Amazon et que vous souhaitez vous connecter avec votre VPC, choisissez Utiliser un VPC et procédez comme suit.

   a. Dans ID du VPC, choisissez votre ID de VPC. Veillez à choisir le VPC de l'infrastructure sur laquelle votre hôte est installé ou un VPC qui a accès à votre instance via VPN ou Direct Connect.

   b. Si vous avez configuré un VPC privé et que vous avez configuré votre hôte pour effectuer la validation TLS à l'aide d'une autorité de certification non publique, dans Certificat TLS, saisissez votre ID de certificat. La valeur du certificat TLS est la clé publique du certificat.
8. Choisissez Create host (Créer un hôte).
9. Une fois la page des détails de l'hôte affichée, l'état de l'hôte change au fur et à mesure que l'hôte est créé.

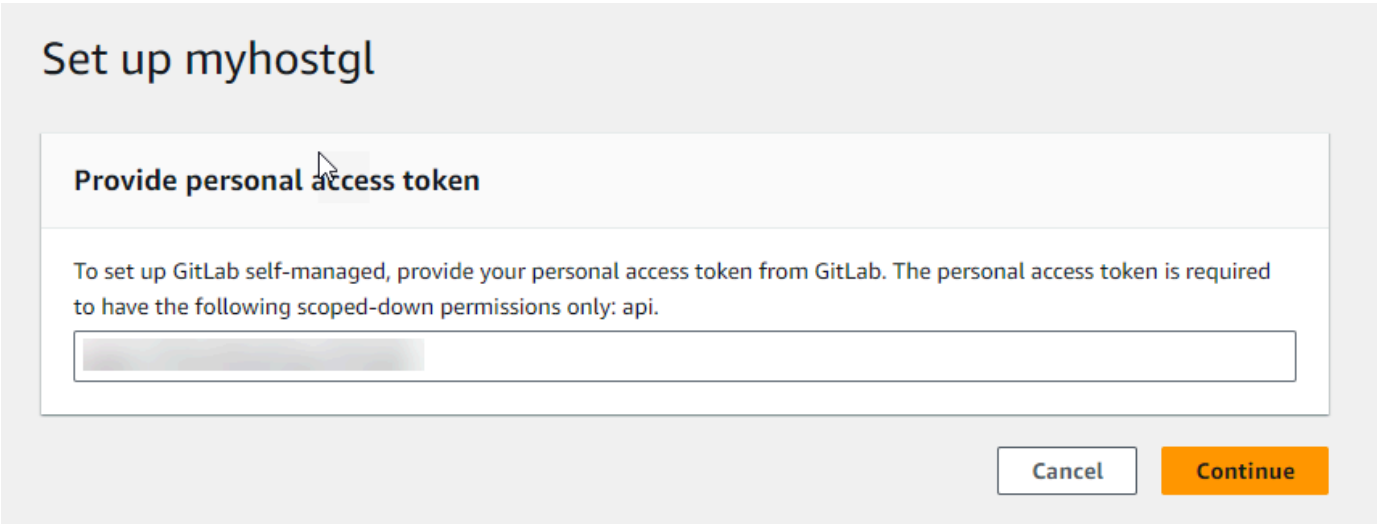
> **Note**
>
> Si la configuration de votre hôte inclut une configuration VPC, prévoyez plusieurs minutes pour l'approvisionnement des composants du réseau hôte.

Attendez que votre hôte atteigne l'état En attente, puis terminez la configuration. Pour plus d'informations, consultez Configurer un hôte en attente.

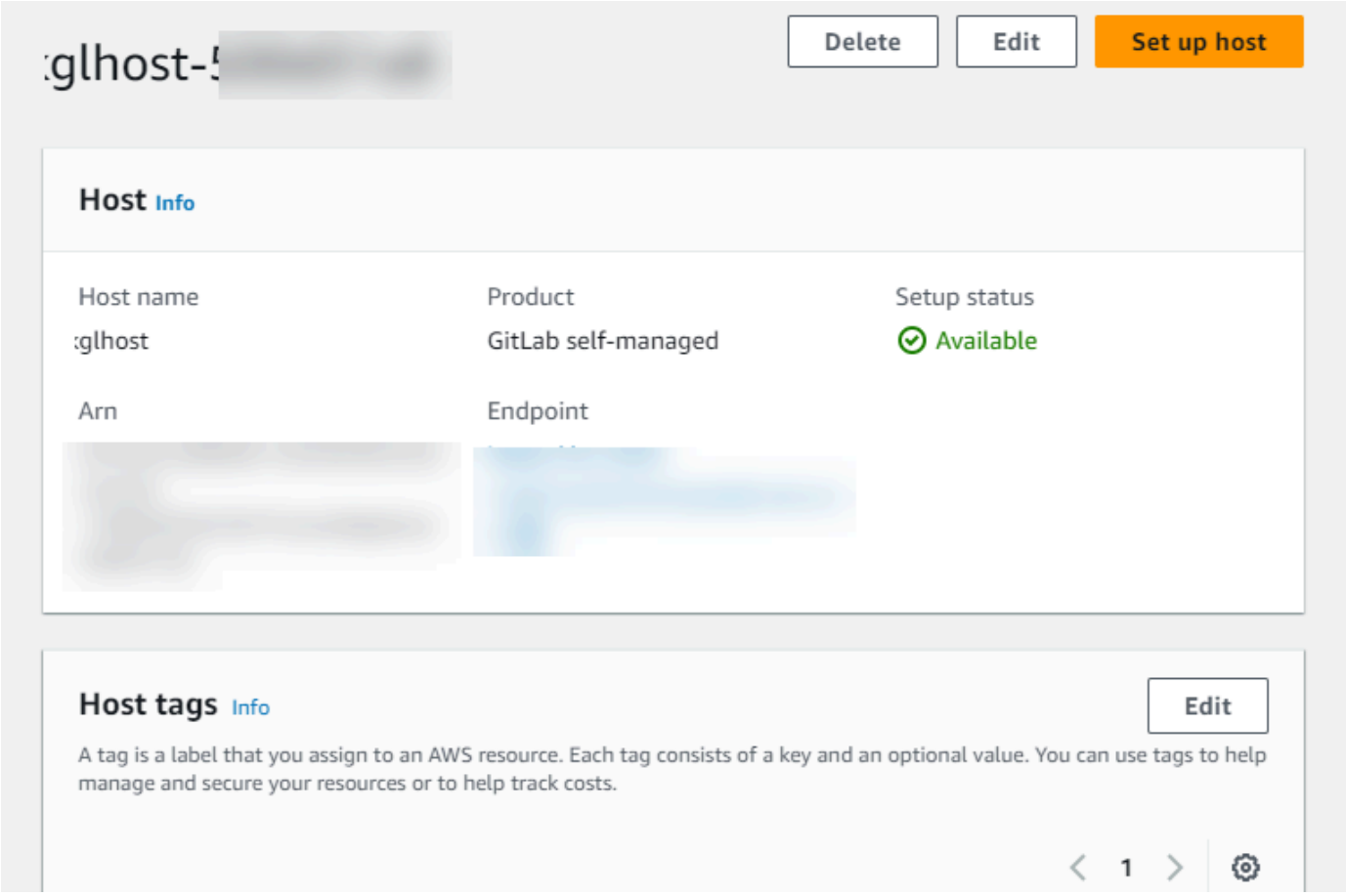


Étape 2 : Configurer votre hôte en attente

1. Choisissez Configurer l'hôte.
2. La page Configurer ***nom_hôte*** s'affiche. Dans Fournir un jeton d'accès personnel, accordez à votre GitLab PAT l'autorisation limitée suivante uniquement : api.

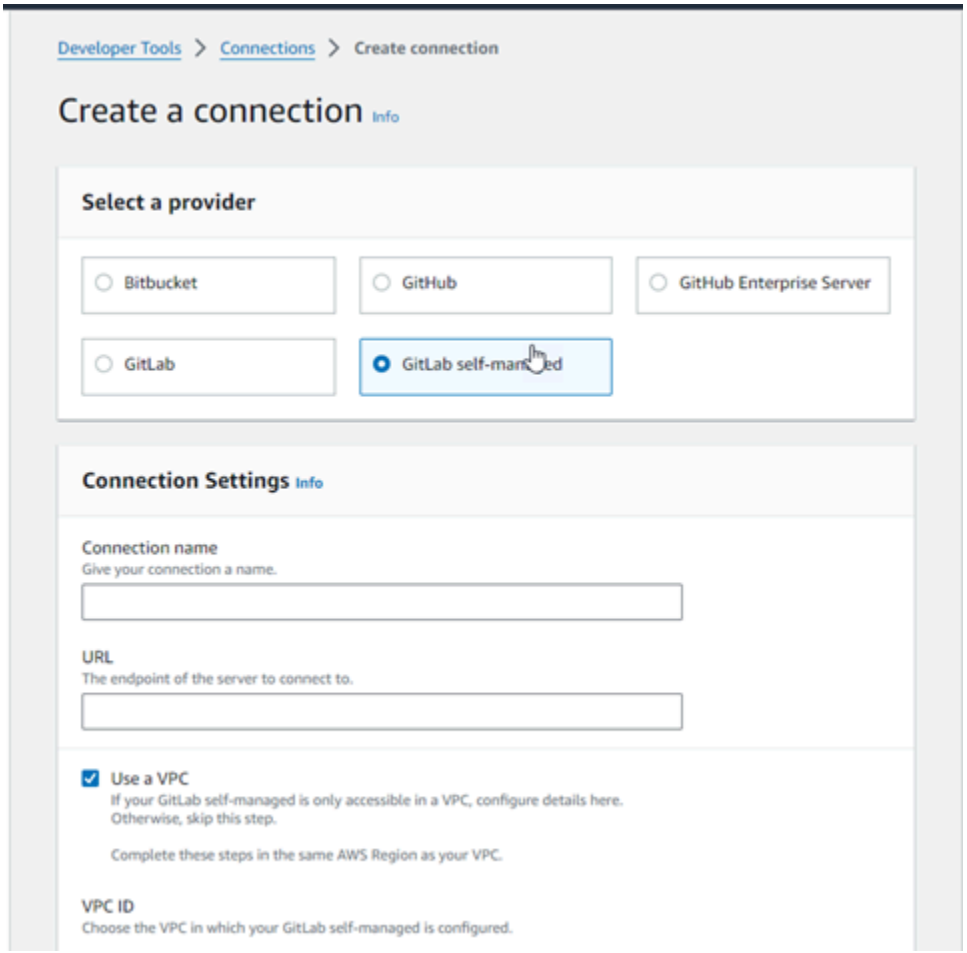


3. Une fois votre hôte enregistré avec succès, la page des détails de l'hôte s'affiche et indique que l'état de l'hôte est Disponible.



Étape 3 : Créer votre connexion

1. Connectez-vous à AWS Management Console, puis ouvrez la console AWS Developer Tools à l'adressehttps://console.aws.amazon.com/codesuite/settings/connections.
2. Choisissez Paramètres, puis choisissez Connexions. Choisissez Créer une connexion.
3. Pour créer une connexion à un GitLab référentiel, sous Sélectionnez un fournisseur, choisissez GitLab Autogéré. Dans Connection name (Nom de la connexion), saisissez le nom de la connexion que vous souhaitez créer.



4. Dans URL, saisissez le point de terminaison de votre serveur.
5. Si vous avez lancé votre serveur dans un VPC Amazon et que vous souhaitez vous connecter à votre VPC, choisissez Use a VPC (Utilisation d'un VPC) et complétez ce qui suit.

   a. Dans ID du VPC, choisissez votre ID de VPC. Veillez à choisir le VPC de l'infrastructure sur laquelle votre hôte est installé ou un VPC qui a accès à votre hôte via VPN ou Direct Connect.

   b. Sous Subnet ID (ID de sous-réseau), choisissez Add (Ajouter). Dans le champ, choisissez l'ID de sous-réseau que vous souhaitez utiliser pour votre hôte. Vous pouvez choisir jusqu'à 10 sous-réseaux.

      Veillez à choisir le sous-réseau de l'infrastructure sur laquelle votre hôte est installé ou un sous-réseau qui a accès à votre hôte installé via VPN ou Direct Connect.

   c. Sous Security group IDs (ID de groupe de sécurité), choisissez Add (Ajouter). Dans le champ, choisissez le groupe de sécurité que vous souhaitez utiliser pour votre hôte. Vous pouvez choisir jusqu'à 10 groupes de sécurité.

Veillez à choisir le groupe de sécurité de l'infrastructure sur laquelle votre hôte est installé ou un groupe de sécurité qui a accès à votre hôte installé via VPN ou Direct Connect.

d. Si vous avez configuré un VPC privé et que vous avez configuré votre hôte pour effectuer la validation TLS à l'aide d'une autorité de certification non publique, dans Certificat TLS, saisissez votre ID de certificat. La valeur du certificat TLS doit être la clé publique du certificat.

6. Choisissez Connect to GitLab self-managed. La connexion créée s'affiche avec le statut En attente. Une ressource hôte est créée pour la connexion avec les informations de serveur que vous avez fournies. Pour le nom d'hôte, l'URL est utilisée.
7. Choisissez Update pending connection (Mettre à jour la connexion en attente).
8. Lorsque la page de connexion GitLab s'affiche, connectez-vous avec vos informations d'identification, puis choisissez Se connecter.
9. Une page d'autorisation s'affiche avec un message demandant l'autorisation de connexion pour accéder à votre GitLab compte.

   Choisissez Authorize (Autoriser).
10. Le navigateur revient à la page de la console des connexions. Sous Créer une GitLab connexion, la nouvelle connexion est affichée dans Nom de la connexion.
11. Choisissez Connect to GitLab self-managed.

    Une fois la connexion créée avec succès, une bannière de réussite s'affiche. Les détails de la connexion sont affichés sur la page Paramètres de connexion.

Création d'une connexion à une interface GitLab autogérée (CLI)

Vous pouvez utiliser le AWS Command Line Interface (AWS CLI) pour créer un hôte et une connexion à des fins GitLab d'autogestion.

Pour ce faire, utilisez les commandes create-host et create-connection.

> **Important**
>
> Une connexion créée via le AWS CLI ou AWS CloudFormation est en `PENDING` état par défaut. Après avoir créé une connexion à l'aide de la CLI AWS CloudFormation, utilisez la console pour modifier la connexion afin de définir son état`AVAILABLE`.

Étape 1 : Pour créer un hôte GitLab autogéré (CLI)

1. Ouvrez une invite de terminal (Linux, macOS ou Unix) ou de commande (Windows). Utilisez le AWS CLI pour exécuter la create-host commande, en spécifiant le `--name``--provider-type`, et `--provider-endpoint` pour votre connexion. Dans cet exemple, le nom du fournisseur tiers est `GitLabSelfManaged` et le point de terminaison est `my-instance.dev`.

   ```
   aws codestar-connections create-host --name MyHost --provider-type
    GitLabSelfManaged --provider-endpoint "https://my-instance.dev"
   ```

   En cas de succès, cette commande renvoie les informations Amazon Resource Name (ARN) hôte semblables à ce qui suit.

   ```
   {
       "HostArn": "arn:aws:codestar-connections:us-west-2:account_id:host/My-
   Host-28aef605"
   }
   ```

   Après cette étape, l'hôte présente l'état `PENDING`.
2. Utilisez la console pour terminer la configuration de l'hôte et le faire passer à l'état `Available`.

Étape 2 : Configurer un hôte en attente dans la console

1. Connectez-vous à la console Developer Tools AWS Management Console et ouvrez-la à l'adressehttps://console.aws.amazon.com/codesuite/settings/connections.
2. Utilisez la console pour terminer la configuration de l'hôte et passer l'hôte vers l'état `Available`. veuillez consulter Configurer un hôte en attente.

Étape 3 : Pour créer une connexion pour l' GitLab autogestion (CLI)

1. Ouvrez une invite de terminal (Linux, macOS ou Unix) ou de commande (Windows). Utilisez le AWS CLI pour exécuter la create-connection commande, en spécifiant le `--host-arn` et `--connection-name` pour votre connexion.

   ```
   aws codestar-connections create-connection --host-arn arn:aws:codestar-
   connections:us-west-2:account_id:host/MyHost-234EXAMPLE --connection-name
    MyConnection
   ```

En cas de succès, cette commande renvoie les informations ARN de connexion semblables à ce qui suit.

```
{
    "ConnectionArn": "arn:aws:codestar-connections:us-west-2:account_id:connection/
aEXAMPLE-8aad"
}
```

2. Utilisez la console pour configurer la connexion en attente à l'étape suivante.

Étape 4 : Pour terminer une connexion pour l' GitLab autogestion dans la console

1. Connectez-vous à la console Developer Tools AWS Management Console et ouvrez-la à l'adressehttps://console.aws.amazon.com/codesuite/settings/connections.
2. Utilisez la console pour configurer la connexion en attente et la faire passer à l'état `Available`. Pour plus d'informations, consultez Mettre à jour une connexion en attente.

Mettre à jour une connexion en attente

Une connexion créée via le AWS Command Line Interface (AWS CLI) ou dont le `PENDING` statut AWS CloudFormation est défini par défaut. Après avoir créé une connexion avec le AWS CLI ou AWS CloudFormation, utilisez la console pour mettre à jour la connexion afin de définir son état`AVAILABLE`.

> **Note**
>
> Vous devez utiliser la console pour mettre à jour la connexion en attente. Vous ne pouvez pas mettre à jour une connexion en attente à l'aide de la AWS CLI.

La première fois que vous utilisez la console pour ajouter une nouvelle connexion à un fournisseur tiers, vous devez établir la liaison OAuth avec le fournisseur tiers en utilisant l'installation associée à votre connexion.

Vous pouvez utiliser la console Outils pour développeurs afin d'établir une connexion en attente.

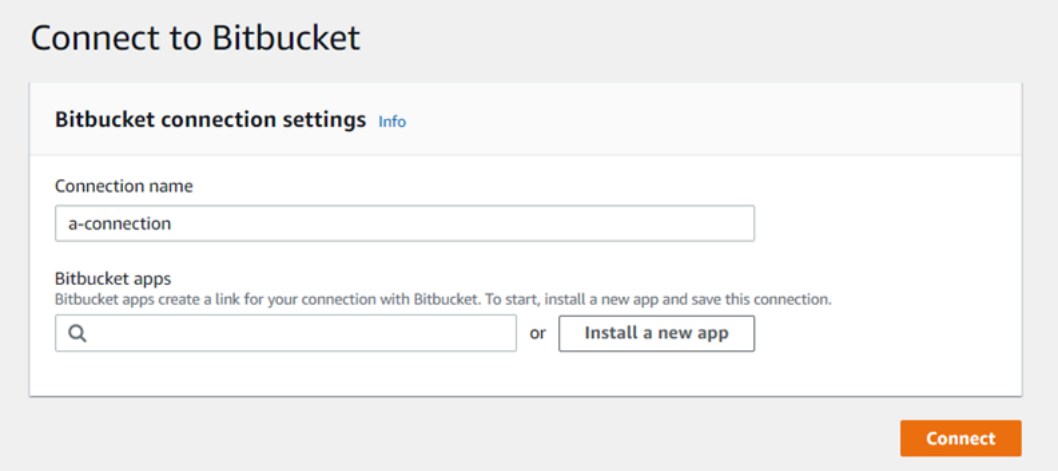
Pour établir une connexion

1. Ouvrez la console AWS Developer Tools à l'adressehttps://console.aws.amazon.com/codesuite/settings/connections.
2. Choisissez Settings > Connections (Paramètres > Connexions).

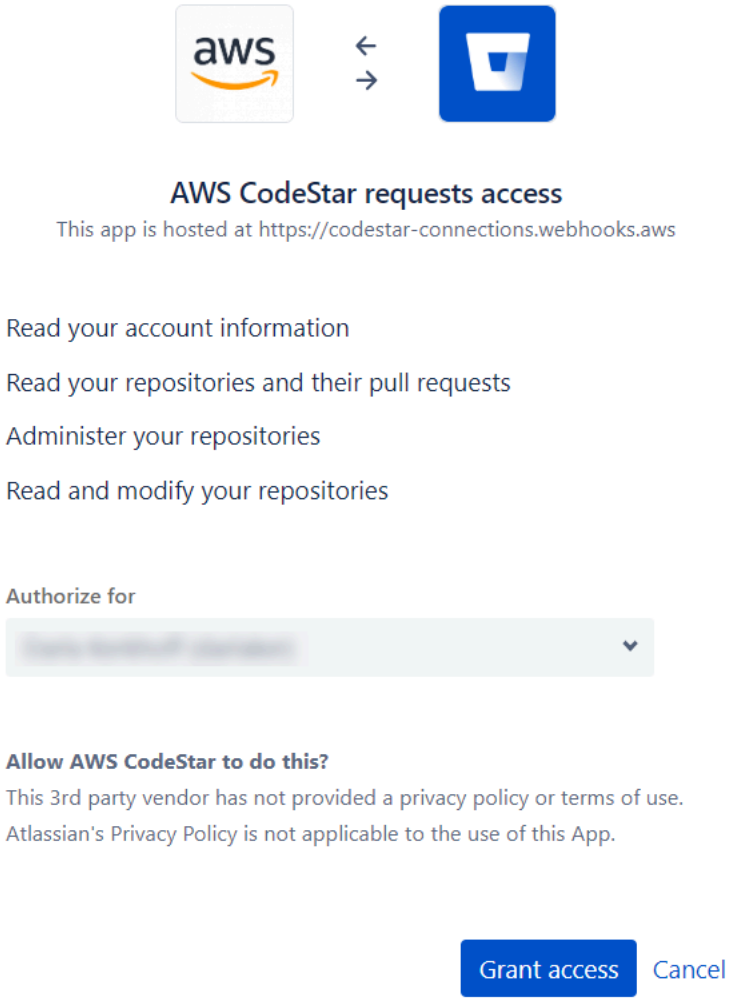
   Les noms de toutes les connexions associées à votre AWS compte sont affichés.
3. Dans Nom, choisissez le nom de la connexion en attente à mettre à jour.

   Update a pending connection (Mettre à jour une connexion en attente) est activé lorsque vous choisissez une connexion avec un statut En attente.
4. Choisissez Update a pending connection (Mettre à jour une connexion en attente).
5. Sur la page Se connecter à Bitbucket, dans Connection name (Nom de la connexion), vérifiez le nom de votre connexion.

   Sous Bitbucket apps (Applications Bitbucket), choisissez une installation d'application ou choisissez Install a new app (Installer une nouvelle application) pour en créer une.



6. Sur la page d'installation de l'application, un message indique que l' AWS CodeStar application essaie de se connecter à votre compte Bitbucket. Choisissez Grant access (Accorder l'accès).



7. L'ID de connexion de votre nouvelle installation s'affiche. Choisissez Complete connection (Terminer la connexion).

Affichage de la liste des connexions

Vous pouvez utiliser la console Outils pour développeurs ou la commande list-connections de AWS Command Line Interface (AWS CLI) pour afficher la liste des connexions de votre compte.

Affichage de la liste des connexions (console)

Pour répertorier les connexions

1. Ouvrez la console Outils pour développeurs à l'adresse https://console.aws.amazon.com/codesuite/settings/connections.
2. Choisissez Settings > Connections (Paramètres > Connexions).

3. Affichez le nom, l'état et l'ARN de vos connexions.

Affichage de la liste des connexions (CLI)

Vous pouvez utiliser le AWS CLI pour répertorier vos connexions à des référentiels de code tiers. Pour une connexion associée à une ressource hôte, telle que les connexions à GitHub Enterprise Server, la sortie renvoie également l'ARN de l'hôte.

Pour ce faire, utilisez la commande list-connections.

Pour répertorier les connexions

- Ouvrez un terminal (Linux, macOS ou Unix) ou une invite de commande (Windows), puis utilisez le AWS CLI pour exécuter la list-connections commande.

```
aws codestar-connections list-connections --provider-type Bitbucket
--max-results 5 --next-token: next-token
```

Cette commande renvoie la sortie suivante.

```
{
     "Connections": [
         {
             "ConnectionName": "my-connection",
             "ProviderType": "Bitbucket",
             "Status": "PENDING",
             "ARN": "arn:aws:codestar-connections:us-west-2:account_id:connection/
aEXAMPLE-8aad-4d5d-8878-dfcab0bc441f",
             "OwnerAccountId": "account_id"
         },
         {
             "ConnectionName": "my-other-connection",
             "ProviderType": "Bitbucket",
             "Status": "AVAILABLE",
             "ARN": "arn:aws:codestar-connections:us-west-2:account_id:connection/
aEXAMPLE-8aad-4d5d-8878-dfcab0bc441f",
             "OwnerAccountId": "account_id"
          },
      ],
     "NextToken": "next-token"
}
```

Supprimer une connexion

Vous pouvez utiliser la console Outils pour développeurs ou la commande delete-connection du AWS Command Line Interface (AWS CLI) pour supprimer une connexion.

Rubriques

- Suppression d'une connexion (console)
- Suppression d'une connexion (CLI)

Suppression d'une connexion (console)

Pour supprimer une connexion

1. Ouvrez la console Outils pour développeurs à l'adresse https://console.aws.amazon.com/codesuite/settings/connections.
2. Choisissez Settings > Connections (Paramètres > Connexions).
3. Dans Nom de la connexion, choisissez le nom de la connexion à supprimer.
4. Sélectionnez Delete (Supprimer).
5. Saisissez **`delete`** dans le champ pour confirmer, puis choisissez Supprimer.

> **Important**
>
> Cette action ne peut pas être annulée.

Suppression d'une connexion (CLI)

Vous pouvez utiliser le AWS Command Line Interface (AWS CLI) pour supprimer une connexion.

Pour ce faire, utilisez la commande delete-connection.

> **Important**
>
> Une fois que vous avez exécuté la commande, la connexion est supprimée. Aucune boîte de dialogue de confirmation ne s'affiche. Vous pouvez créer une nouvelle connexion, mais l'ARN (Amazon Resource Name) n'est jamais réutilisé.

Pour supprimer une connexion

- Ouvrez une invite de terminal (Linux, macOS ou Unix) ou de commande (Windows). Utilisez le AWS CLI pour exécuter la delete-connection commande, en spécifiant l'ARN de la connexion que vous souhaitez supprimer.

  ```
  aws codestar-connections delete-connection --connection-arn arn:aws:codestar-
  connections:us-west-2:account_id:connection/aEXAMPLE-8aad-4d5d-8878-dfcab0bc441f
  ```

  Cette commande ne donne aucun résultat.

Balisage des ressources de connexions

Une balise est une étiquette d'attribut personnalisée que vous attribuez ou AWS assignez à une AWS ressource. Chaque AWS étiquette comporte deux parties :

- Une clé de balise (par exemple, `CostCenter`, `Environment` ou `Project`). Les clés de balises sont sensibles à la casse.
- Un champ facultatif appelé valeur de balise (par exemple, `111122223333`, `Production` ou le nom d'une équipe). Omettre la valeur de balise équivaut à l'utilisation d'une chaîne vide. Les valeurs de balise sont sensibles à la casse, tout comme les clés de balise.

Ensemble, ces informations sont qualifiées de paires clé-valeur.

Vous pouvez utiliser la console ou la CLI pour baliser des ressources.

Vous pouvez baliser les types de ressources suivants dans CodeConnections :

- Connexions
- Hôtes

Ces étapes supposent que vous avez déjà installé une version récente AWS CLI ou que vous avez déjà mis à jour la version actuelle. Pour plus d'informations, consultez Installation d' AWS CLI dans le Guide de l'utilisateur AWS Command Line Interface .

Outre l'identification, l'organisation et le suivi de votre ressource à l'aide de balises, vous pouvez utiliser des balises dans les politiques AWS Identity and Access Management (IAM) pour contrôler qui peut consulter votre ressource et interagir avec elle. Pour obtenir des exemples de stratégies

d'accès basées sur les balises, consultez Utilisation de balises pour contrôler l'accès aux ressources AWS CodeStar Connections.

Rubriques

- Ressources de balisage (console)
- Étiqueter des ressources (CLI)

Ressources de balisage (console)

Vous pouvez utiliser la console pour ajouter, mettre à jour ou supprimer des balises sur une ressource de connexion.

Rubriques

- Ajouter des balises à une ressource de connexion (console)
- Affichage des balises d'une ressource de connexion (console)
- Modifier les balises d'une ressource de connexion (console)
- Supprimer des balises d'une ressource de connexion (console)

Ajouter des balises à une ressource de connexion (console)

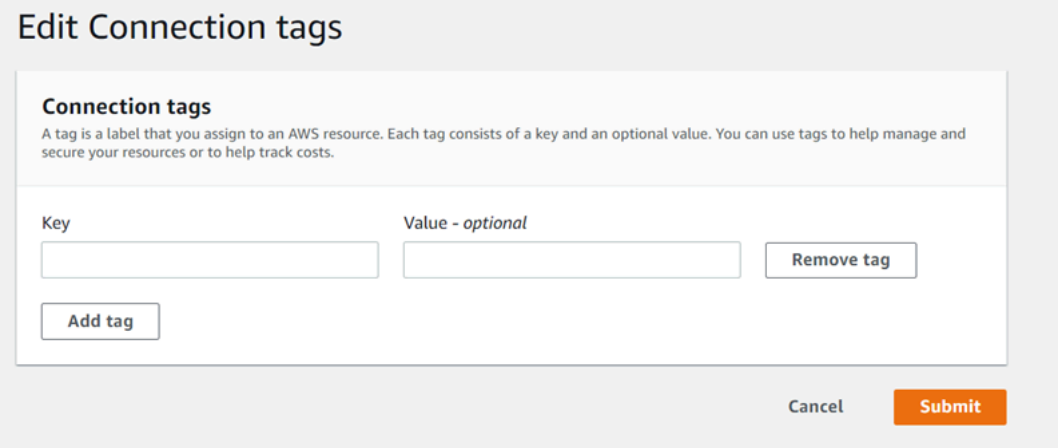
Vous pouvez utiliser la console pour ajouter des balises à une connexion ou un hôte existant.

> **Note**
>
> Lorsque vous créez une connexion pour un fournisseur installé tel qu' GitHubEnterprise Server, et qu'une ressource hôte est également créée pour vous, les balises lors de la création sont ajoutées à la connexion uniquement. Cela vous permet d'étiqueter un hôte séparément si vous souhaitez le réutiliser pour une nouvelle connexion. Si vous souhaitez ajouter des balises à l'hôte, suivez les étapes ci-dessous.

Pour ajouter des balises à une connexion

1. Connectez-vous à la console. Choisissez Paramètres dans le volet de navigation.
2. Sous Settings (Paramètres), choisissez Connections (Connexions). Choisissez l'onglet Connections (Connexions).

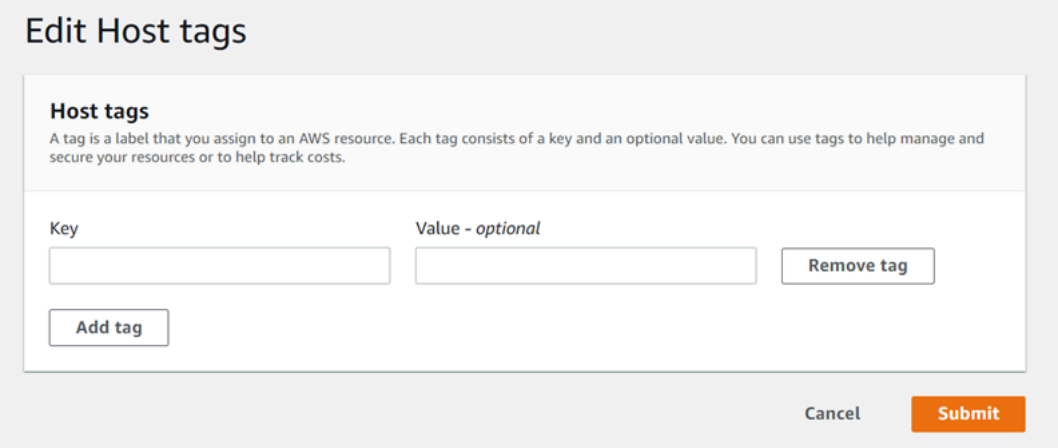
3. Choisissez la connexion que vous souhaitez modifier. La page des paramètres de connexion s'affiche.
4. Sous Connection tags (Balises de connexion), choisissez Edit (Modifier). La page Modifier les balises de connexion s'affiche.
5. Dans les champs Clé et Valeur, entrez une paire de clés pour chaque ensemble de balises que vous souhaitez ajouter. (Le champ Valeur est facultatif.) Par exemple, dans Clé, saisissez **`Project`**. Dans Value (Valeur), entrez **`ProjectA`**.



6. (Facultatif) Choisissez Add tag (Ajouter une balise) pour ajouter d'autres lignes et saisir d'autres balises.
7. Sélectionnez Envoyer. Les balises sont répertoriées sous les paramètres de connexion.

Pour ajouter des balises à un hôte

1. Connectez-vous à la console. Choisissez Paramètres dans le volet de navigation.
2. Sous Settings (Paramètres), choisissez Connections (Connexions). Cliquez sur l'onglet Hosts (Hôtes).
3. Choisissez l'hôte que vous voulez modifier. La page des paramètres d'hôte s'affiche.
4. Sous Host tags (Balises d'hôte), choisissez Edit (Modifier). La page Balises d'hôte s'affiche.
5. Dans les champs Clé et Valeur, entrez une paire de clés pour chaque ensemble de balises que vous souhaitez ajouter. (Le champ Valeur est facultatif.) Par exemple, dans Clé, saisissez **`Project`**. Dans Value (Valeur), entrez **`ProjectA`**.



6. (Facultatif) Choisissez Add tag (Ajouter une balise) pour ajouter d'autres lignes et saisir d'autres balises pour un hôte.
7. Sélectionnez Envoyer. Les balises sont répertoriées sous les paramètres d'hôte.

Affichage des balises d'une ressource de connexion (console)

Vous pouvez utiliser la console pour afficher les balises des ressources existantes.

Pour ajouter les balises d'une connexion

1. Connectez-vous à la console. Choisissez Paramètres dans le volet de navigation.
2. Sous Settings (Paramètres), choisissez Connections (Connexions). Choisissez l'onglet Connections (Connexions).
3. Choisissez la connexion que vous souhaitez afficher. La page des paramètres de connexion s'affiche.
4. Sous Connection tags (Balises de connexion), affichez les balises de connexion dans les colonnes Key (Clé) et Value (Valeur).

Pour afficher les balises d'un hôte

1. Connectez-vous à la console. Choisissez Paramètres dans le volet de navigation.
2. Sous Settings (Paramètres), choisissez Connections (Connexions). Cliquez sur l'onglet Hosts (Hôtes).
3. Choisissez l'hôte que vous souhaitez afficher.
4. Sous Host tags (Balises d'hôte), affichez les balises d'hôte dans les colonnes Key (Clé) et Value (Valeur).

Modifier les balises d'une ressource de connexion (console)

Vous pouvez utiliser la console pour modifier les balises qui ont été ajoutées aux ressources de connexion.

Pour modifier les balises d'une connexion

1. Connectez-vous à la console. Choisissez Paramètres dans le volet de navigation.
2. Sous Settings (Paramètres), choisissez Connections (Connexions). Choisissez l'onglet Connections (Connexions).
3. Choisissez la connexion que vous souhaitez modifier. La page des paramètres de connexion s'affiche.
4. Sous Connection tags (Balises de connexion), choisissez Edit (Modifier). La page Balises de connexion s'affiche.
5. Dans les champs Clé et Valeur, mettez à jour les valeurs dans chaque champ selon vos besoins. Par exemple, pour la clé **`Project`**, dans Valeur, remplacez **`ProjectA`** par **`ProjectB`**.
6. Sélectionnez Envoyer.

Pour modifier les balises d'un hôte

1. Connectez-vous à la console. Choisissez Paramètres dans le volet de navigation.
2. Sous Settings (Paramètres), choisissez Connections (Connexions). Cliquez sur l'onglet Hosts (Hôtes).
3. Choisissez l'hôte que vous voulez modifier. La page des paramètres d'hôte s'affiche.
4. Sous Host tags (Balises d'hôte), choisissez Edit (Modifier). La page Balises d'hôte s'affiche.
5. Dans les champs Clé et Valeur, mettez à jour les valeurs dans chaque champ selon vos besoins. Par exemple, pour la clé **`Project`**, dans Valeur, remplacez **`ProjectA`** par **`ProjectB`**.
6. Sélectionnez Envoyer.

Supprimer des balises d'une ressource de connexion (console)

Vous pouvez utiliser la console pour supprimer des balises des ressources de connexion. Lorsque vous supprimez des balises de la ressource associée, les balises sont supprimées.

Pour supprimer les balises d'une connexion

1. Connectez-vous à la console. Choisissez Paramètres dans le volet de navigation.
2. Sous Settings (Paramètres), choisissez Connections (Connexions). Choisissez l'onglet Connections (Connexions).
3. Choisissez la connexion que vous souhaitez modifier. La page des paramètres de connexion s'affiche.
4. Sous Connection tags (Balises de connexion), choisissez Edit (Modifier). La page Balises de connexion s'affiche.
5. En regard de la clé et de la valeur de chaque balise que vous souhaitez supprimer, choisissez Supprimer la balise.
6. Sélectionnez Envoyer.

Pour supprimer les balises d'un hôte

1. Connectez-vous à la console. Choisissez Paramètres dans le volet de navigation.
2. Sous Settings (Paramètres), choisissez Connections (Connexions). Cliquez sur l'onglet Hosts (Hôtes).
3. Choisissez l'hôte que vous voulez modifier. La page des paramètres d'hôte s'affiche.
4. Sous Host tags (Balises d'hôte), choisissez Edit (Modifier). La page Balises d'hôte s'affiche.
5. En regard de la clé et de la valeur de chaque balise que vous souhaitez supprimer, choisissez Supprimer la balise.
6. Sélectionnez Envoyer.

Étiqueter des ressources (CLI)

Vous pouvez utiliser la CLI pour consulter, ajouter, mettre à jour ou supprimer des balises sur une ressource de connexion.

Rubriques

- Ajouter des balises à une ressource de connexion (CLI)
- Affichage des balises d'une ressource de connexions (CLI)
- Modification des balises d'une ressource de connexion (CLI)
- Supprimer des balises d'une ressource de connexion (CLI)

Ajouter des balises à une ressource de connexion (CLI)

Vous pouvez utiliser le AWS CLI pour étiqueter les ressources dans les connexions.

Depuis le terminal ou la ligne de commande, exécutez la commande tag-resource, en spécifiant l'ARN (Amazon Resource Name) de la ressource dans laquelle vous souhaitez ajouter des balises, ainsi que la clé et la valeur de la balise que vous souhaitez ajouter. Vous pouvez ajouter plusieurs balises.

Pour ajouter des balises à une connexion

1. Obtenez l'ARN pour votre ressource. Utilisation de la commande list-connections affichée dans Affichage de la liste des connexions pour obtenir l'ARN de connexion.
2. Dans le terminal ou la ligne de commande, exécutez la commande tag-resource.

   Par exemple, utilisez la commande suivante pour baliser une connexion avec deux balises, une clé de balise nommée Project avec la valeur de balise ProjectA et une clé de balise nommée ReadOnlyavec la valeur de balise true.

   ```
   aws codestar-connections tag-resource --resource-arn arn:aws:codestar-
   connections:us-west-2:account_id:connection/aEXAMPLE-8aad-4d5d-8878-dfcab0bc441f --
   tags Key=Project,Value=ProjectA Key=IscontainerBased,Value=true
   ```

   Si elle aboutit, cette commande ne renvoie rien.

Pour ajouter des balises à un hôte

1. Obtenez l'ARN pour votre ressource. Utilisation de la commande list-hosts affichée dans Liste des hôtes pour obtenir l'ARN d'hôte
2. Dans le terminal ou la ligne de commande, exécutez la commande tag-resource.

   Par exemple, utilisez la commande suivante pour étiqueter un hôte avec deux balises, une clé de balise nommée Project avec la valeur de balise ProjectA et une clé de balise nommée IscontainerBasedavec la valeur de balise true.

```
aws codestar-connections tag-resource --resource-arn arn:aws:codestar-
connections:us-west-2:account_id:host/My-Host-28aef605 --tags
 Key=Project,Value=ProjectA Key=IscontainerBased,Value=true
```

Si elle aboutit, cette commande ne renvoie rien.

Affichage des balises d'une ressource de connexions (CLI)

Vous pouvez utiliser le AWS CLI pour afficher les AWS balises d'une ressource de connexion. Si aucune balise n'a été ajoutée, la liste renvoyée est vide. Utilisation de la commande list-tags-for-resource pour afficher les balises qui ont été ajoutées à une connexion ou à un hôte.

Pour ajouter les balises d'une connexion

1. Obtenez l'ARN pour votre ressource. Utilisation de la commande list-connections affichée dans Affichage de la liste des connexions pour obtenir l'ARN de connexion.
2. Dans le terminal ou la ligne de commande, exécutez la commande list-tags-for-resource. Par exemple, utilisez la commande suivante pour afficher une liste de clés de balise et de valeurs de balise pour une connexion.

```
aws codestar-connections list-tags-for-resource --resource-arn arn:aws:codestar-
connections:us-west-2:account_id:connection/aEXAMPLE-8aad-4d5d-8878-dfcab0bc441f
```

Cette commande renvoie les balises associées à la ressource. Cet exemple montre deux paires clé/valeur renvoyées pour une connexion.

```
{
    "Tags": [
        {
            "Key": "Project",
            "Value": "ProjectA"
        },
        {
            "Key": "ReadOnly",
            "Value": "true"
        }
    ]
}
```

Pour afficher les balises d'un hôte

1. Obtenez l'ARN pour votre ressource. Utilisation de la commande list-hosts affichée dans Liste des hôtes pour obtenir l'ARN d'hôte
2. Dans le terminal ou la ligne de commande, exécutez la commande list-tags-for-resource. Par exemple, utilisez la commande suivante pour afficher une liste de clés de balise et de valeurs de balise pour un hôte.

   ```
   aws codestar-connections list-tags-for-resource --resource-arn arn:aws:codestar-connections:us-west-2:account_id:host/My-Host-28aef605
   ```

   Cette commande renvoie les balises associées à la ressource. Cet exemple montre deux paires clé/valeur renvoyées pour un hôte.

   ```
   {
       "Tags": [
           {
               "Key": "IscontainerBased",
               "Value": "true"
           },
           {
               "Key": "Project",
               "Value": "ProjectA"
           }
       ]
   }
   ```

Modification des balises d'une ressource de connexion (CLI)

Vous pouvez utiliser le AWS CLI pour modifier le tag d'une ressource. Vous pouvez modifier la valeur d'une clé existante ou ajouter une autre clé.

Depuis le terminal ou la ligne de commande, exécutez la commande tag-resource, en spécifiant l'ARN de la ressource dans laquelle vous souhaitez mettre à jour une balise et spécifiez la clé de balise et la valeur de balise à mettre à jour.

Lorsque vous modifiez des balises, toutes les clés de balise non spécifiées seront conservées, tandis que tout ce qui a la même clé, mais une nouvelle valeur sera mis à jour. Les nouvelles clés ajoutées avec la commande de modification sont ajoutées en tant que nouvelle paire clé/valeur.

Pour modifier les balises d'une connexion

1. Obtenez l'ARN pour votre ressource. Utilisation de la commande list-connections affichée dans Affichage de la liste des connexions pour obtenir l'ARN de connexion.
2. Dans le terminal ou la ligne de commande, exécutez la commande tag-resource.

   Dans cet exemple, la valeur de la clé `Project` est remplacée par `ProjectB`.

   ```
   aws codestar-connections tag-resource --resource-arn arn:aws:codestar-
   connections:us-west-2:account_id:connection/aEXAMPLE-8aad-4d5d-8878-dfcab0bc441f --
   tags Key=Project,Value=ProjectB
   ```

   Si elle aboutit, cette commande ne renvoie rien. Pour vérifier quelles balises sont associées à la connexion, exécutez la commande list-tags-for-resource.

Pour modifier les balises d'un hôte

1. Obtenez l'ARN pour votre ressource. Utilisation de la commande list-hosts affichée dans Liste des hôtes pour obtenir l'ARN d'hôte
2. Dans le terminal ou la ligne de commande, exécutez la commande tag-resource.

   Dans cet exemple, la valeur de la clé `Project` est remplacée par `ProjectB`.

   ```
   aws codestar-connections tag-resource --resource-arn arn:aws:codestar-
   connections:us-west-2:account_id:host/My-Host-28aef605 --tags
    Key=Project,Value=ProjectB
   ```

   Si elle aboutit, cette commande ne renvoie rien. Pour vérifier quelles balises sont associées à l'hôte, exécutez la commande list-tags-for-resource.

Supprimer des balises d'une ressource de connexion (CLI)

Procédez comme suit pour utiliser le AWS CLI pour supprimer une balise d'une ressource. Lorsque vous supprimez des balises de la ressource associée, les balises sont supprimées.

> **Note**
>
> Si vous supprimez une ressource de connexions, toutes les associations de balises sont effacées de la ressource supprimée. Vous n'avez pas besoin d'effacer les balises avant de supprimer une ressource de connexion.

Depuis le terminal ou la ligne de commande, exécutez la commande untag-resource, en spécifiant l'ARN de la ressource dans laquelle vous souhaitez supprimer des balises et la clé de balise de la balise que vous souhaitez supprimer. Par exemple, pour supprimer plusieurs balises sur une connexion à l'aide des touches de balise *Project* et *ReadOnly*, utilisez la commande suivante.

```
aws codestar-connections untag-resource --resource-arn arn:aws:codestar-connections:us-
west-2:account_id:connection/aEXAMPLE-8aad-4d5d-8878-dfcab0bc441f --tag-
keys Project ReadOnly
```

Si elle aboutit, cette commande ne renvoie rien. Pour vérifier les balises associées à la ressource, exécutez la commande list-tags-for-resource. La sortie indique que toutes les balises ont été supprimées.

```
{
    "Tags": []
}
```

Affichage des informations de connexion

Vous pouvez utiliser la console Outils pour développeurs ou la commande get-connection du AWS Command Line Interface (AWS CLI) pour afficher les détails d'une connexion. Pour utiliser le AWS CLI, vous devez avoir déjà installé une version récente du AWS CLI ou avoir mis à jour la version actuelle. Pour de plus amples informations, consultez Installation d' AWS CLI dans le Guide de l'utilisateur AWS Command Line Interface .

Pour afficher une connexion (console)

1. Ouvrez la console Outils pour développeurs à l'adresse https://console.aws.amazon.com/codesuite/settings/connections.
2. Choisissez Settings > Connections (Paramètres > Connexions).

3. Cliquez sur le bouton en regard de la connexion que vous souhaitez afficher, puis choisissez View details (Afficher les détails).
4. Les informations suivantes s'affichent pour votre connexion :

   - Le nom de la connexion.
   - Le type de fournisseur de votre connexion.
   - Le statut de la connexion.
   - L'ARN de connexion.
   - Si la connexion a été créée pour un fournisseur installé, tel qu' GitHubEnterprise Server, les informations d'hôte associées à la connexion.
   - Si la connexion a été créée pour un fournisseur installé, tel qu' GitHubEnterprise Server, les informations de point de terminaison associées à l'hôte pour la connexion.
5. Si la connexion est En attente, pour établir la connexion, choisissez Update pending connection (Mettre à jour la connexion en attente). Pour de plus amples informations, consultez Mettre à jour une connexion en attente.

Pour afficher une connexion (CLI)

- Depuis le terminal ou la ligne de commande, exécutez la commande get-connection. Par exemple, utilisez la commande suivante pour afficher les détails d'une connexion avec la valeur d'ARN `arn:aws:codestar-connections:us-west-2:account_id:connection/aEXAMPLE-8aad-4d5d-8878-dfcab0bc441f`.

  ```
  aws codestar-connections get-connection --connection-arn arn:aws:codestar-connections:us-west-2:account_id:connection/aEXAMPLE-8aad-4d5d-8878-dfcab0bc441f
  ```

  Si la commande est réussie, elle renvoie les détails de confirmation.

  Exemple de sortie pour une connexion Bitbucket :

  ```
  {
      "Connection": {
          "ConnectionName": "MyConnection",
          "ConnectionArn": "arn:aws:codestar-connections:us-west-2:account_id:connection/cdacd948-EXAMPLE",
          "ProviderType": "Bitbucket",
          "OwnerAccountId": "account_id",
  ```

```
        "ConnectionStatus": "AVAILABLE"
    }
}
```

Exemple de sortie pour une GitHub connexion :

```
{
    "Connection": {
        "ConnectionName": "MyGitHubConnection",
        "ConnectionArn": "arn:aws:codestar-connections:us-
west-2:account_id:connection/ebcd4a13-EXAMPLE",
        "ProviderType": "GitHub",
        "OwnerAccountId": "account_id",
        "ConnectionStatus": "AVAILABLE"
    }
}
```

Exemple de sortie pour une connexion GitHub Enterprise Server :

```
{
    "Connection": {
        "ConnectionName": "MyConnection",
        "ConnectionArn": "arn:aws:codestar-connections:us-
west-2:account_id:connection/2d178fb9-EXAMPLE",
        "ProviderType": "GitHubEnterpriseServer",
        "OwnerAccountId": "account_id",
        "ConnectionStatus": "PENDING",
        "HostArn": "arn:aws:codestar-connections:us-west-2:account_id:host/sdfsdf-
EXAMPLE"
    }
}
```

Utilisation d'hôtes

Pour créer une connexion à un type de fournisseur installé, tel que GitHub Enterprise Server, vous devez d'abord créer un hôte à l'aide de la AWS Management Console. Un hôte est une ressource que vous créez pour représenter l'infrastructure sur laquelle votre fournisseur est installé. Ensuite, vous créez une connexion à l'aide de cet hôte. Pour de plus amples informations, veuillez consulter Utilisation des connexions.

Par exemple, vous créez un hôte pour votre connexion afin que l'application tierce de votre fournisseur puisse être enregistrée pour représenter votre infrastructure. Vous créez un hôte pour un type de fournisseur, puis toutes vos connexions à ce type de fournisseur utilisent cet hôte.

Lorsque vous utilisez la console pour créer une connexion à un type de fournisseur installé, tel que GitHub Enterprise Server, la console crée la ressource hôte pour vous.

Rubriques

Création d'un hôte

Vous pouvez utiliser la AWS Management Console ou la AWS Command Line Interface(AWS CLI) pour créer une connexion à un référentiel de code tiers installé sur votre infrastructure. Par exemple, GitHub Enterprise Server peut être exécuté en tant que machine virtuelle sur une instance Amazon EC2. Avant de créer une connexion à GitHub Enterprise Server, créez un hôte à utiliser pour la connexion.

Pour voir une présentation du flux de travail de création d'hôte pour les fournisseurs installés, consultez Flux de travail de création ou de mise à jour d'un hôte.

Avant de commencer :

- (Facultatif) Si vous souhaitez créer votre hôte avec un VPC, vous devez déjà avoir créé un réseau ou un cloud privé virtuel (VPC).
- Vous devez déjà avoir créé votre instance et, si vous prévoyez de vous connecter à votre VPC, avoir lancé votre hôte dans votre VPC.

> **Note**
>
> Chaque VPC ne peut être associé qu'à un seul hôte à la fois.

Vous pouvez éventuellement configurer votre hôte avec un VPC. Pour plus d'informations sur la configuration réseau et de VPC pour votre ressource hôte, consultez les prérequis pour les VPC dans (Facultatif) Prérequis : configuration réseau ou d'Amazon VPC pour votre connexion et Résolution des problèmes liés à la configuration d'un VPC pour votre hôte.

Pour utiliser la console pour créer un hôte et une connexion à GitHub Enterprise Server, consultez Créez votre connexion au serveur GitHub d'entreprise (console). La console crée un hôte pour vous.

Pour utiliser la console pour créer un hôte et une connexion à GitLab autogéré, consultez Création d'une connexion à l' GitLabautogestion. La console crée un hôte pour vous.

(Facultatif) Prérequis : configuration réseau ou d'Amazon VPC pour votre connexion

Si votre infrastructure est configurée avec une connexion réseau, vous pouvez ignorer cette section.

Si votre hôte est uniquement accessible dans un VPC, suivez ces exigences de VPC avant de continuer.

Exigences du VPC

Vous pouvez éventuellement choisir de créer votre hôte avec un VPC. Vous trouverez ci-dessous les exigences générales du VPC, en fonction du VPC que vous avez configuré pour votre installation.

- Vous pouvez configurer un VPC public avec des sous-réseaux publics et privés. Vous pouvez utiliser le VPC par défaut pour votre Compte AWS si vous n'avez pas de sous-réseaux ou de blocs d'adresse CIDR préférés.
- Si vous avez configuré un VPC privé et que vous avez configuré votre instance GitHub Enterprise Server pour effectuer la validation TLS à l'aide d'une autorité de certification non publique, vous devez fournir le certificat TLS pour votre ressource hôte.
- Lorsque les connexions AWS CodeStar créent votre hôte, le point de terminaison de VPC (PrivateLink) pour webhooks est créé automatiquement. Pour de plus amples informations, veuillez consulter AWS CodeStar Connections et points de terminaison de VPC d'interface (AWS PrivateLink).
- Configuration du groupe de sécurité :
  - Les groupes de sécurité utilisés lors de la création de l'hôte nécessitent des règles entrantes et sortantes qui permettent à l'interface réseau de se connecter à votre instance GitHub Enterprise Server

  - Les groupes de sécurité attachés à votre instance GitHub Enterprise Server (ne faisant pas partie de la configuration de l'hôte) nécessitent un accès entrant et sortant à partir des interfaces réseau créées par les connexions.
- Vos sous-réseaux VPC doivent résider dans des zones de disponibilité différentes dans votre région. Les zones de disponibilité sont des emplacements distincts isolés des défaillances dans d'autres zones de disponibilité. Chaque sous-réseau doit résider entièrement dans une zone de disponibilité et ne peut pas s'étendre sur plusieurs zones.

Pour plus d'informations sur l'utilisation des VPC et des sous-réseaux, veuillez consulter Dimensionnement des VPC et des sous-réseaux pour IPv4 dans le guide de l'utilisateur Amazon VPC.

Informations sur le VPC que vous fournissez pour la configuration de l'hôte

Lorsque vous créez votre ressource hôte pour vos connexions à l'étape suivante, vous devez fournir les éléments suivants :

- ID de VPC : l'ID du VPC du serveur sur lequel votre instance GitHub Enterprise Server est installée ou d'un VPC qui a accès à votre instance GitHub Enterprise Server installée via VPN ou Direct Connect.
- Un ou plusieurs ID de sous-réseau : l'ID du sous-réseau du serveur sur lequel votre instance GitHub Enterprise Server est installée ou d'un sous-réseau qui a accès à votre instance GitHub Enterprise Server installée via VPN ou Direct Connect.
- Un ou plusieurs groupes de sécurité : le groupe de sécurité du serveur sur lequel votre instance GitHub Enterprise Server est installée ou un groupe de sécurité qui a accès à votre instance GitHub Enterprise Server installée via VPN ou Direct Connect.
- Point de terminaison : préparez votre point de terminaison de serveur et passez à l'étape suivante.

Pour plus d'informations, notamment sur la résolution des problèmes de connexion VPC ou hôte, consultez Résolution des problèmes liés à la configuration d'un VPC pour votre hôte.

Conditions d'autorisation

Dans le cadre du processus de création de l'hôte, les connexions AWS CodeStar créent des ressources réseau en votre nom pour faciliter la connectivité VPC. Cela inclut une interface réseau permettant aux connexions AWS Codestar d'interroger les données de votre hôte, et un point de

terminaison de VPC ou PrivateLink permettant à l'hôte d'envoyer des données d'événement aux connexions AWS CodeStar via des webhooks. Pour pouvoir créer ces ressources réseau, veillez à ce que le rôle utilisé pour créer l'hôte dispose des autorisations suivantes :

```
ec2:CreateNetworkInterface
ec2:CreateTags
ec2:DescribeDhcpOptions
ec2:DescribeNetworkInterfaces
ec2:DescribeSubnets
ec2:DeleteNetworkInterface
ec2:DescribeVpcs
ec2:CreateVpcEndpoint
ec2:DeleteVpcEndpoints
ec2:DescribeVpcEndpoints
```

Pour plus d'informations sur la résolution des problèmes d'autorisation ou de connexion hôte dans un VPC, consultez Résolution des problèmes liés à la configuration d'un VPC pour votre hôte.

Pour plus d'informations sur les points de terminaison d'un VPC, webhook, consultez AWS CodeStar Connections et points de terminaison de VPC d'interface (AWS PrivateLink).

Rubriques

- Créer un hôte pour une connexion (console)
- Création d'un hôte pour une connexion (CLI)

Créer un hôte pour une connexion (console)

Pour les connexions pour les installations, par exemple avec GitHub Enterprise Server ou avec GitLab autogéré, vous utilisez un hôte pour représenter le point de terminaison de l'infrastructure sur laquelle votre fournisseur tiers est installé.

Pour en savoir plus sur les considérations relatives à la configuration d'un hôte dans un VPC, consultez Création d'une connexion à l' GitLabautogestion.

Pour utiliser la console pour créer un hôte et une connexion à GitHub Enterprise Server, consultez Créez votre connexion au serveur GitHub d'entreprise (console). La console crée un hôte pour vous.

Pour utiliser la console pour créer un hôte et une connexion à GitLab autogéré, consultez Création d'une connexion à l' GitLabautogestion. La console crée un hôte pour vous.

> **Note**
>
> Vous ne créez un hôte qu'une seule fois par compte GitHub Enterprise Server ou GitLab autogéré. Toutes vos connexions à un compte GitHub Enterprise Server ou GitLab autogéré spécifique utiliseront le même hôte.

Création d'un hôte pour une connexion (CLI)

Vous pouvez utiliser la AWS Command Line Interface (AWS CLI) pour créer un hôte pour les connexions installées.

> **Note**
>
> Vous ne créez un hôte qu'une seule fois par compte GitHub Enterprise Server. Toutes vos connexions à un compte GitHub Enterprise Server spécifique utiliseront le même hôte.

Vous utilisez un hôte pour représenter le point de terminaison de l'infrastructure sur laquelle votre fournisseur tiers est installé. Pour créer un hôte à l'aide de la CLI, utilisez la commande create-host. Une fois que vous avez terminé la création de l'hôte, l'hôte est En attente. Ensuite, configurez l'hôte pour le passer à l'état Disponible. Une fois l'hôte disponible, procédez comme suit pour créer une connexion.

> **Important**
>
> Un hôte créé via la AWS CLI présente l'état `Pending` par défaut. Après avoir créé un hôte avec la CLI, utilisez la console pour configurer l'hôte et définir son état sur `Available`.

Pour utiliser la console pour créer un hôte et une connexion à GitHub Enterprise Server, consultez Créez votre connexion au serveur GitHub d'entreprise (console). La console crée un hôte pour vous.

Pour utiliser la console pour créer un hôte et une connexion à GitLab autogéré, consultez Création d'une connexion à l' GitLabautogestion. La console crée un hôte pour vous.

Configurer un hôte en attente

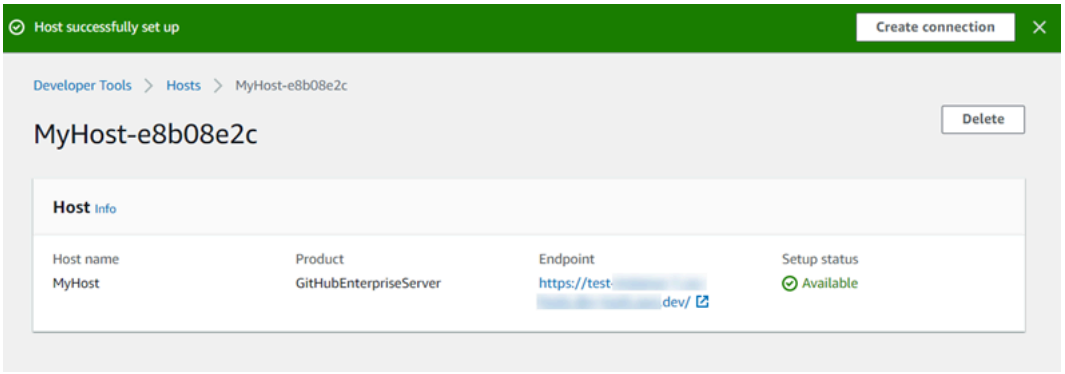
Un hôte créée via la AWS Command Line Interface (AWS CLI) ou le kit SDK présente l'état `Pending` par défaut. Après avoir créé une connexion avec la console, AWS CLI ou le kit SDK, utilisez la console pour configurer l'hôte et définir son état sur `Available`.

Vous devez déjà avoir créé un hôte. Pour plus d'informations, consultez Create a host (Créer un hôte).

Pour configurer un hôte en attente

Une fois votre hôte créé, il présente l'état En attente. Pour passer l'hôte de l'état En attente à Disponible, procédez comme suit. Ce processus entre en négociation avec le fournisseur tiers pour enregistrer l'application de connexion AWS sur l'hôte.

1. Une fois que votre hôte atteint l'état En attente sur la console Outils pour développeurs AWS, choisissez Set up host (Configurer l'hôte).
2. Si vous créez un hôte pour GitLab autogéré, une page Configuration s'affiche. Dans Fournir un jeton d'accès personnel, attribuez à votre PAT GitLab l'autorisation limitée suivante uniquement : api.
3. Sur la page de connexion du fournisseur tiers installé, tel que Serveur GitHub Enterprise, connectez-vous avec les informations d'identification de votre compte si vous y êtes invité.
4. Sur la page d'installation de l'application, dans GitHub App name (Nom de l'appli GitHub), saisissez un nom pour l'application que vous souhaitez installer pour votre hôte. Choisissez Create GitHun App (Créer une application GitHub).
5. Une fois votre hôte enregistré avec succès, la page des détails de l'hôte s'affiche et indique que l'état de l'hôte est Disponible.



6. Vous pouvez continuer à créer votre connexion une fois que l'hôte est disponible. Sur la bannière de réussite, choisissez Create connection (Créer une connexion). Suivez les étapes de Create a connection (Créer une connexion).

Liste des hôtes

Vous pouvez utiliser la console Outils pour développeurs ou la commande list-connections de AWS Command Line Interface (AWS CLI) pour afficher la liste des connexions de votre compte.

Liste des hôtes (console)

Pour répertorier les hôtes

1. Ouvrez la console Outils pour développeurs à l'adresse https://console.aws.amazon.com/codesuite/settings/connections.
2. Cliquez sur l'onglet Hosts (Hôtes). Affichez le nom, l'état et l'ARN de vos hôtes.

Répertorier les hôtes (CLI)

Vous pouvez utiliser la AWS CLI pour répertorier vos hôtes pour les connexions de fournisseurs tiers installés.

Pour ce faire, utilisez la commande list-hosts.

Pour répertorier les hôtes

- Ouvrez une invite de terminal (Linux, macOS, or Unix) ou une invite de commande (Windows) et utilisez la AWS CLI pour exécuter la commande list-hosts.

```
aws codestar-connections list-hosts
```

Cette commande renvoie la sortie suivante.

```
{
    "Hosts": [
        {
            "Name": "My-Host",
            "HostArn": "arn:aws:codestar-connections:us-west-2:account_id:host/My-Host-28aef605",
```

```
            "ProviderType": "GitHubEnterpriseServer",
            "ProviderEndpoint": "https://my-instance.test.dev",
            "Status": "AVAILABLE"
        }
    ]
}
```

Modifier un hôte

Vous pouvez modifier les paramètres d'hôte d'un hôte avec l'état `Pending`. Vous pouvez modifier le nom d'hôte, l'URL ou la configuration du VPC.

Vous ne pouvez pas utiliser la même URL pour plusieurs hôtes.

> **Note**
>
> Pour en savoir plus sur les considérations relatives à la configuration d'un hôte dans un VPC, consultez (Facultatif) Prérequis : configuration réseau ou d'Amazon VPC pour votre connexion.

Pour modifier un hôte

1. Ouvrez la console Outils pour développeurs à l'adresse https://console.aws.amazon.com/codesuite/settings/connections.
2. Choisissez Settings > Connections (Paramètres > Connexions).
3. Cliquez sur l'onglet Hosts (Hôtes).

   Les hôtes associés à votre compte AWS et créés dans la région AWS associée sont affichés.
4. Pour modifier le nom d'hôte, saisissez une nouvelle valeur dans Name (Nom).
5. Pour modifier le point de terminaison d'hôte, saisissez une nouvelle valeur dans URL.
6. Pour modifier la configuration du VPC hôte, saisissez de nouvelles valeurs dans VPC ID (ID de VPC).
7. Choisissez Edit host (Modifier l'hôte).
8. Les paramètres mis à jour s'affichent. Choisissez Set up Pending host (Configurer l'hôte en attente).

Supprimer un hôte

Vous pouvez utiliser la console Outils pour développeurs ou la commande delete-host de la AWS Command Line Interface (AWS CLI) pour supprimer un hôte.

Rubriques

Supprimer un hôte (console)

Pour supprimer un hôte

1. Ouvrez la console Outils pour développeurs à l'adresse https://console.aws.amazon.com/codesuite/settings/connections.
2. Cliquez sur l'onglet Hosts (Hôtes). Dans Name (Nom), choisissez le nom de l'hôte que vous souhaitez supprimer.
3. Sélectionnez Delete.
4. Saisissez **`delete`** dans le champ pour confirmer, puis choisissez Supprimer.

> **Important**
>
> Cette action ne peut pas être annulée.

Supprimer un hôte (CLI)

Vous pouvez utiliser la AWS Command Line Interface (AWS CLI) pour supprimer un hôte.

Pour ce faire, utilisez la commande delete-host.

> **Important**
>
> Avant de pouvoir supprimer un hôte, vous devez supprimer toutes les connexions associées à l'hôte.
> Une fois que vous avez exécuté la commande, l'hôte est supprimé. Aucune boîte de dialogue de confirmation ne s'affiche.

Pour supprimer un hôte

- Ouvrez une invite de terminal (Linux, macOS ou Unix) ou de commande (Windows). Utilisez la AWS CLI pour exécuter la commande delete-host, en spécifiant l'Amazon Resource Name (ARN) de l'hôte que vous souhaitez supprimer.

  ```
  aws codestar-connections delete-host --host-arn "arn:aws:codestar-connections:us-west-2:account_id:host/My-Host-28aef605"
  ```

  Cette commande ne donne aucun résultat.

Afficher les détails de l'hôte

Vous pouvez utiliser la console Outils pour développeurs ou la commande get-host de la AWS Command Line Interface (AWS CLI) pour afficher les détails d'un hôte.

Pour afficher les détails de l'hôte (console)

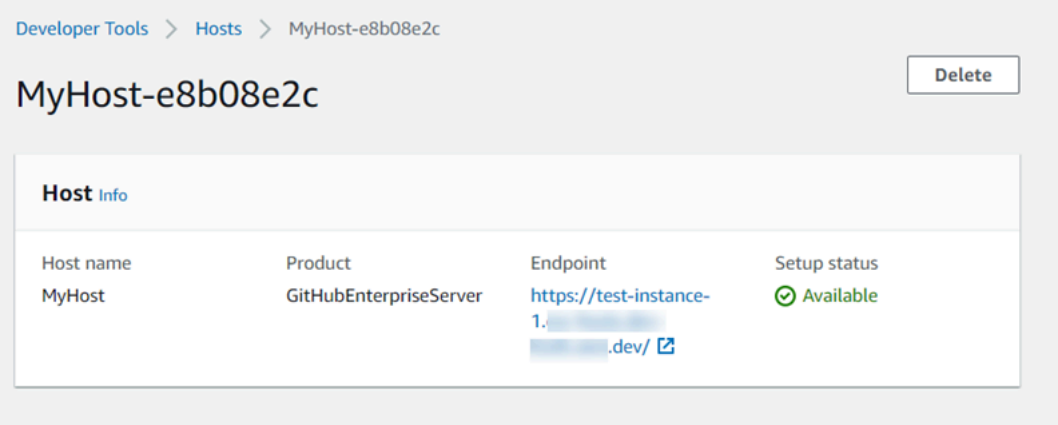
1. Connectez-vous à la AWS Management Console et ouvrez la console Outils pour développeurs à l'adresse https://console.aws.amazon.com/codesuite/settings/connections.
2. Choisissez Settings > Connections (Paramètres > Connexions), puis choisissez l'onglet Hosts (hôtes).
3. Cliquez sur le bouton en regard de l'hôte que vous souhaitez afficher, puis choisissez View details (Afficher les détails).
4. Les informations suivantes s'affichent pour votre hôte :

   - Le nom de l'hôte.
   - Le type de fournisseur de votre connexion.
   - Le point de terminaison de l'infrastructure sur laquelle votre fournisseur est installé.
   - L'état de configuration de votre hôte. Un hôte prêt pour une connexion présente l'état Disponible. Si votre hôte a été créé, mais que la configuration n'est pas terminée, l'hôte peut présenter un état différent.

     Les états disponibles sont les suivants :

     - EN ATTENTE : l'hôte a terminé la création et est prêt à démarrer la configuration en enregistrant l'application fournisseur sur l'hôte.

- DISPONIBLE : l'hôte a terminé la création et la configuration et est disponible pour une utilisation avec les connexions.
- ERREUR : une erreur s'est produite lors de la création ou de l'enregistrement de l'hôte.
- VPC_CONFIG_VPC_INITIALISATION : la configuration du VPC pour l'hôte est en cours de création.
- VPC_CONFIG_VPC_FAILED_INITIALISATION : la configuration du VPC pour l'hôte a rencontré une erreur et a échoué.
- VPC_CONFIG_VPC_AVAILLEUR : la configuration du VPC de l'hôte a terminé la configuration et est disponible.
- VPC_CONFIG_VPC_DELETING : la configuration du VPC de l'hôte est en cours de suppression.



5. Pour supprimer l'hôte, choisissez Delete (Supprimer).
6. Si l'hôte présente l'état En attente, pour terminer la configuration, choisissez Set up host (Configurer l'hôte). Pour de plus amples informations, consultez Configurer un hôte en attente.

Pour afficher les détails de l'hôte (CLI)

- Ouvrez une invite de terminal (Linux, macOS ou Unix) ou une invite de commande (Windows) et utilisez la AWS CLI pour exécuter la commande get-host en spécifiant l'Amazon Resource Name (ARN) de l'hôte pour lequel vous voulez afficher les détails.

```
aws codestar-connections get-host --host-arn arn:aws:codestar-connections:us-
west-2:account_id:host/My-Host-28aef605
```

Cette commande renvoie la sortie suivante.

```
{
    "Name": "MyHost",
    "Status": "AVAILABLE",
    "ProviderType": "GitHubEnterpriseServer",
    "ProviderEndpoint": "https://test-instance-1.dev/"
}
```

Utilisation des configurations de synchronisation pour les référentiels liés

Dans AWS CodeStar Connections, vous utilisez une connexion pour associer AWS des ressources à un référentiel tiers GitHub, tel que Bitbucket Cloud, GitHub Enterprise Server et GitLab. À l'aide du type de `CFN_STACK_SYNC` synchronisation, vous pouvez créer une configuration de synchronisation qui permet de AWS synchroniser le contenu d'un dépôt Git pour mettre à jour une AWS ressource spécifiée. AWS CloudFormation s'intègre aux connexions afin que vous puissiez utiliser Git sync pour gérer vos fichiers de modèles et de paramètres dans un référentiel lié avec lequel vous vous synchronisez.

Après avoir créé une connexion, vous pouvez utiliser la CLI des connexions ou la AWS CloudFormation console pour créer le lien de votre référentiel et synchroniser la configuration.

- Lien de référentiel : un lien de référentiel crée une association entre votre connexion et un référentiel Git externe. Le lien de référentiel permet à la synchronisation Git de surveiller et de synchroniser les modifications apportées aux fichiers dans un référentiel Git spécifié.
- Configuration de synchronisation : utilisez la configuration de synchronisation pour synchroniser le contenu d'un dépôt Git afin de mettre à jour une AWS ressource spécifiée.

Pour plus d'informations, consultez la référence de l'API AWS CodeStar Connections.

Pour un didacticiel expliquant comment créer une configuration de synchronisation pour une AWS CloudFormation pile à l'aide de la AWS CloudFormation console, consultez la section Utilisation de la synchronisation AWS CloudFormation Git dans le guide de CloudFormation l'utilisateur.

Rubriques

- Utilisation des liens de référentiel
- Utilisation des configurations de synchronisation

Utilisation des liens de référentiel

Un lien de référentiel crée une association entre votre connexion et un référentiel Git externe. Le lien vers le dépôt permet à Git sync de surveiller et de synchroniser les modifications apportées aux fichiers d'un dépôt Git spécifié avec une AWS CloudFormation pile.

Pour plus d'informations sur les liens vers les référentiels, consultez la référence de l'API AWS CodeStar Connections.

Rubriques

Création d'un lien de référentiel

Vous pouvez utiliser la create-repository-link commande dans le AWS Command Line Interface (AWS CLI) pour créer un lien entre votre connexion et le référentiel externe avec lequel vous souhaitez effectuer la synchronisation.

Avant de pouvoir créer un lien vers un référentiel, vous devez déjà avoir créé votre référentiel externe auprès de votre fournisseur tiers, par exemple GitHub.

Pour créer un lien de référentiel

1. Ouvrez une invite de terminal (Linux, macOS ou Unix) ou de commande (Windows). Utilisez le AWS CLI pour exécuter la create-repository-link commande. Spécifiez l'ARN de la connexion associée, l'ID du propriétaire et le nom du référentiel.

   ```
   aws codestar-connections create-repository-link --connection-arn  arn:aws:codestar-connections:us-east-1:account_id:connection/001f5be2-a661-46a4-b96b-4d277cac8b6e --owner-id account_id --repository-name MyRepo
   ```

2. Cette commande renvoie la sortie suivante.

   ```
   {
       "RepositoryLinkInfo": {
   ```

```
        "ConnectionArn": "arn:aws:codestar-connections:us-
east-1:account_id:connection/aEXAMPLE-8aad-4d5d-8878-dfcab0bc441f",
        "OwnerId": "account_id",
        "ProviderType": "GitHub",
        "RepositoryLinkArn": "arn:aws:codestar-connections:us-
east-1:account_id:repository-link/be8f2017-b016-4a77-87b4-608054f70e77",
        "RepositoryLinkId": "be8f2017-b016-4a77-87b4-608054f70e77",
        "RepositoryName": "MyRepo",
        "Tags": []
    }
}
```

Mise à jour d'un lien de référentiel

Vous pouvez utiliser la update-repository-link commande dans le AWS Command Line Interface (AWS CLI) pour mettre à jour un lien de dépôt spécifié.

Vous pouvez mettre à jour les informations suivantes pour votre lien de référentiel :

- `--connection-arn`
- `--owner-id`
- `--repository-name`

Vous pouvez mettre à jour un lien de référentiel lorsque vous souhaitez modifier la connexion associée à votre référentiel. Pour utiliser une autre connexion, vous devez spécifier l'ARN de la connexion. Pour connaître les étapes permettant d'afficher l'ARN de votre connexion, consultez Affichage des informations de connexion.

Pour mettre à jour un lien de référentiel

1. Ouvrez une invite de terminal (Linux, macOS ou Unix) ou de commande (Windows). Utilisez le AWS CLI pour exécuter la update-repository-link commande, en spécifiant la valeur à mettre à jour pour le lien du référentiel. Par exemple, la commande suivante met à jour la connexion associée à l'ID du lien de référentiel. Elle spécifie le nouvel ARN de connexion avec le paramètre `--connection`.

```
aws codestar-connections update-repository-link --repository-link-id
 6053346f-8a33-4edb-9397-10394b695173 --connection-arn arn:aws:codestar-
connections:us-east-1:account_id:connection/aEXAMPLE-f055-4843-adef-4ceaefcb2167
```

2. Cette commande renvoie la sortie suivante.

```
{
    "RepositoryLinkInfo": {
        "ConnectionArn": "arn:aws:codestar-connections:us-
east-1:account_id:connection/aEXAMPLE-f055-4843-adef-4ceaefcb2167",
        "OwnerId": "owner_id",
        "ProviderType": "GitHub",
        "RepositoryLinkArn": "arn:aws:codestar-connections:us-
east-1:account_id:repository-link/6053346f-8a33-4edb-9397-10394b695173",
        "RepositoryLinkId": "6053346f-8a33-4edb-9397-10394b695173",
        "RepositoryName": "MyRepo",
        "Tags": []
    }
}
```

Liste des liens de référentiel

Vous pouvez utiliser la list-repository-links commande dans le AWS Command Line Interface (AWS CLI) pour répertorier les liens du référentiel de votre compte.

Pour répertorier des liens de référentiel

1. Ouvrez une invite de terminal (Linux, macOS ou Unix) ou de commande (Windows). Utilisez le AWS CLI pour exécuter la list-repository-links commande.

```
aws codestar-connections list-repository-links
```

2. Cette commande renvoie la sortie suivante.

```
{
    "RepositoryLinks": [
        {
            "ConnectionArn": "arn:aws:codestar-connections:us-
east-1:account_id:connection/001f5be2-a661-46a4-b96b-4d277cac8b6e",
            "OwnerId": "owner_id",
            "ProviderType": "GitHub",
            "RepositoryLinkArn": "arn:aws:codestar-connections:us-
east-1:account_id:repository-link/6053346f-8a33-4edb-9397-10394b695173",
            "RepositoryLinkId": "6053346f-8a33-4edb-9397-10394b695173",
            "RepositoryName": "MyRepo",
```

```
            "Tags": []
        }
    ]
}
```

Suppression d'un lien de référentiel

Vous pouvez utiliser la delete-repository-link commande dans le AWS Command Line Interface (AWS CLI) pour supprimer un lien vers un dépôt.

Avant de pouvoir supprimer un lien de référentiel, vous devez supprimer toutes les configurations de synchronisation associées à ce lien de référentiel.

> **Important**
>
> Une fois que vous avez exécuté la commande, le lien de référentiel est supprimé. Aucune boîte de dialogue de confirmation ne s'affiche. Vous pouvez créer un nouveau lien de référentiel, mais l'Amazon Resource Name (ARN) n'est pas réutilisé.

Pour supprimer un lien de référentiel

- Ouvrez une invite de terminal (Linux, macOS ou Unix) ou de commande (Windows). Utilisez le AWS CLI pour exécuter la delete-repository-link commande, en spécifiant l'ID du lien du référentiel à supprimer.

  ```
  aws codestar-connections delete-repository-link --repository-link-id
   6053346f-8a33-4edb-9397-10394b695173
  ```

  Cette commande ne donne aucun résultat.

Affichage des détails d'un lien de référentiel

Vous pouvez utiliser la get-repository-link commande dans le AWS Command Line Interface (AWS CLI) pour afficher les détails d'un lien vers un dépôt.

Pour afficher les détails d'un lien de référentiel

1. Ouvrez une invite de terminal (Linux, macOS ou Unix) ou de commande (Windows). Utilisez le AWS CLI pour exécuter la get-repository-link commande, en spécifiant l'ID du lien du référentiel.

```
aws codestar-connections get-repository-link --repository-link-id
 6053346f-8a33-4edb-9397-10394b695173
```

2. Cette commande renvoie la sortie suivante.

```
{
    "RepositoryLinkInfo": {
        "ConnectionArn": "arn:aws:codestar-connections:us-
east-1:account_id:connection/aEXAMPLE-8aad-4d5d-8878-dfcab0bc441f",
        "OwnerId": "owner_id",
        "ProviderType": "GitHub",
        "RepositoryLinkArn": "arn:aws:codestar-connections:us-
east-1:account_id:repository-link/be8f2017-b016-4a77-87b4-608054f70e77",
        "RepositoryLinkId": "6053346f-8a33-4edb-9397-10394b695173",
        "RepositoryName": "MyRepo",
        "Tags": []
    }
}
```

Utilisation des configurations de synchronisation

Une configuration de synchronisation crée une association entre un référentiel et une connexion spécifiés. Utilisez la configuration de synchronisation pour synchroniser le contenu d'un référentiel Git afin de mettre à jour une ressource AWS spécifiée.

Pour plus d'informations sur les connexions, consultez la référence de l'API AWS CodeStar Connections.

Rubriques

- Création d'une configuration de synchronisation
- Mise à jour d'une configuration de synchronisation
- Liste des configurations de synchronisation
- Suppression d'une configuration de synchronisation

- Affichage des détails d'une configuration de synchronisation

Création d'une configuration de synchronisation

Vous pouvez utiliser la create-repository-link commande dans le AWS Command Line Interface (AWS CLI) pour créer un lien entre votre connexion et le référentiel externe avec lequel vous souhaitez effectuer la synchronisation.

Avant de créer une configuration de synchronisation, vous devez déjà avoir créé un lien de référentiel entre votre connexion et votre référentiel tiers.

Pour créer une configuration de synchronisation

1. Ouvrez une invite de terminal (Linux, macOS ou Unix) ou de commande (Windows). Utilisez le AWS CLI pour exécuter la create-repository-link commande. Spécifiez l'ARN de la connexion associée, l'ID du propriétaire et le nom du référentiel. La commande suivante crée une configuration de synchronisation avec un type de synchronisation pour une ressource dans AWS CloudFormation. Elle spécifie également la branche du référentiel et le fichier de configuration du référentiel. Dans cet exemple, la ressource est une pile nommée **`mystack`**.

```
aws codestar-connections create-sync-configuration --branch main --config-file
 filename --repository-link-id be8f2017-b016-4a77-87b4-608054f70e77 --resource-name
 mystack --role-arn arn:aws:iam::account_id:role/myrole --sync-type CFN_STACK_SYNC
```

2. Cette commande renvoie la sortie suivante.

```
{
    "SyncConfiguration": {
        "Branch": "main",
        "ConfigFile": "filename",
        "OwnerId": "account_id",
        "ProviderType": "GitHub",
        "RepositoryLinkId": "be8f2017-b016-4a77-87b4-608054f70e77",
        "RepositoryName": "MyRepo",
        "ResourceName": "mystack",
        "RoleArn": "arn:aws:iam::account_id:role/myrole",
        "SyncType": "CFN_STACK_SYNC"
    }
```

Mise à jour d'une configuration de synchronisation

Vous pouvez utiliser la commande update-sync-configuration dans l' AWS Command Line Interface (AWS CLI) pour mettre à jour une configuration de synchronisation spécifiée.

Vous pouvez mettre à jour les informations suivantes pour votre configuration de synchronisation :

- `--branch`
- `--config-file`
- `--repository-link-id`
- `--resource-name`
- `--role-arn`

Pour mettre à jour une configuration de synchronisation

1. Ouvrez une invite de terminal (Linux, macOS ou Unix) ou de commande (Windows). Utilisez le AWS CLI pour exécuter la update-sync-configuration commande, en spécifiant la valeur que vous souhaitez mettre à jour, ainsi que le nom de la ressource et le type de synchronisation. Par exemple, la commande suivante met à jour le nom de branche associé à la configuration de synchronisation avec le paramètre `--branch`.

   ```
   aws codestar-connections update-sync-configuration --sync-type CFN_STACK_SYNC --
   resource-name mystack --branch feature-branch
   ```

2. Cette commande renvoie la sortie suivante.

   ```
   {
       "SyncConfiguration": {
           "Branch": "feature-branch",
           "ConfigFile": "filename.yaml",
           "OwnerId": "owner_id",
           "ProviderType": "GitHub",
           "RepositoryLinkId": "6053346f-8a33-4edb-9397-10394b695173",
           "RepositoryName": "MyRepo",
           "ResourceName": "mystack",
           "RoleArn": "arn:aws:iam::account_id:role/myrole",
           "SyncType": "CFN_STACK_SYNC"
       }
   ```

Liste des configurations de synchronisation

Vous pouvez utiliser la commande list-sync-configurations dans l' AWS Command Line Interface (AWS CLI) pour répertorier les liens de référentiel de votre compte.

Pour répertorier des liens de référentiel

1. Ouvrez une invite de terminal (Linux, macOS ou Unix) ou de commande (Windows). Utilisez le AWS CLI pour exécuter la list-sync-configurations commande, en spécifiant le type de synchronisation et l'ID du lien du référentiel.

```
aws codestar-connections list-sync-configurations --repository-link-id
 6053346f-8a33-4edb-9397-10394b695173  --sync-type CFN_STACK_SYNC
```

2. Cette commande renvoie la sortie suivante.

```
{
    "SyncConfigurations": [
        {
            "Branch": "main",
            "ConfigFile": "filename.yaml",
            "OwnerId": "owner_id",
            "ProviderType": "GitHub",
            "RepositoryLinkId": "6053346f-8a33-4edb-9397-10394b695173",
            "RepositoryName": "MyRepo",
            "ResourceName": "mystack",
            "RoleArn": "arn:aws:iam::account_id:role/myrole",
            "SyncType": "CFN_STACK_SYNC"
        }
    ]
}
```

Suppression d'une configuration de synchronisation

Vous pouvez utiliser la commande delete-sync-configuration dans l' AWS Command Line Interface (AWS CLI) pour supprimer une configuration de synchronisation.

> **Important**
>
> Une fois que vous avez exécuté la commande, la configuration de synchronisation est supprimée. Aucune boîte de dialogue de confirmation ne s'affiche. Vous pouvez créer une

nouvelle configuration de synchronisation, mais l'Amazon Resource Name (ARN) n'est pas réutilisé.

Pour supprimer une configuration de synchronisation

- Ouvrez une invite de terminal (Linux, macOS ou Unix) ou de commande (Windows). Utilisez le AWS CLI pour exécuter la delete-sync-configuration commande, en spécifiant le type de synchronisation et le nom de ressource pour la configuration de synchronisation que vous souhaitez supprimer.

  ```
  aws codestar-connections delete-sync-configuration --sync-type CFN_STACK_SYNC --
  resource-name mystack
  ```

  Cette commande ne donne aucun résultat.

Affichage des détails d'une configuration de synchronisation

Vous pouvez utiliser la get-sync-configuration commande dans le AWS Command Line Interface (AWS CLI) pour afficher les détails d'une configuration de synchronisation.

Pour afficher les détails d'une configuration de synchronisation

1. Ouvrez une invite de terminal (Linux, macOS ou Unix) ou de commande (Windows). Utilisez le AWS CLI pour exécuter la get-sync-configuration commande, en spécifiant l'ID du lien du référentiel.

   ```
   aws codestar-connections get-sync-configuration --sync-type CFN_STACK_SYNC --
   resource-name mystack
   ```

2. Cette commande renvoie la sortie suivante.

   ```
   {
       "SyncConfiguration": {
           "Branch": "main",
           "ConfigFile": "filename",
           "OwnerId": "owner_id",
           "ProviderType": "GitHub",
           "RepositoryLinkId": "be8f2017-b016-4a77-87b4-608054f70e77",
           "RepositoryName": "MyRepo",
   ```

```
        "ResourceName": "mystack",
        "RoleArn": "arn:aws:iam::account_id:role/myrole",
        "SyncType": "CFN_STACK_SYNC"
    }
}
```

Journalisation des appels d'API AWS CodeConnections avec AWS CloudTrail

AWS CodeConnections est intégré avec AWS CloudTrail, un service qui fournit un enregistrement des actions entreprises par un utilisateur, un rôle ou un service AWS. CloudTrail capture les appels d'API pour les notifications en tant qu'événements. Les appels capturées incluent des appels de la console Developer Tools et le code des appels vers les opérations d'API AWS CodeConnections.

Si vous créez un journal d'activité, vous pouvez activer la livraison continue des événements CloudTrail dans un compartiment Amazon Simple Storage Service (Amazon S3, y compris les événements pour les notifications. Si vous ne configurez pas de journal d'activité, vous pouvez toujours afficher les événements les plus récents dans la console CloudTrail dans Event history (Historique des événements). En utilisant les informations collectées par CloudTrail, vous pouvez déterminer la demande qui a été envoyée à AWS CodeConnections, l'adresse IP d'où la demande a émané, l'auteur et la date de la demande, ainsi que d'autres détails.

Pour plus d'informations, consultez le AWS CloudTrailGuide de l'utilisateur .

AWS CodeConnections Informations dans CloudTrail

CloudTrail est activé dans votre compte AWS lors de sa création. Lorsqu'une activité a lieu dans AWS CodeConnections, cette activité est enregistrée dans un événement CloudTrail avec d'autres AWS événements de service dans Historique des événements. Vous pouvez afficher, rechercher et télécharger les événements récents dans votre AWS compte. Pour plus d'informations, consultez la section Affichage des événements avec l'historique des événements CloudTrail dans le AWS CloudTrailGuide de l'utilisateur.

Pour enregistrer en continu les événements dans votre compte AWS, y compris les événements d'AWS CodeConnections, créez un journal d'activité. Un journal d'activité permet à CloudTrail de distribuer les fichiers journaux vers Simple Storage Service (Amazon S3) bucket. Par défaut, lorsque vous créez un journal d'activité dans la console, il s'applique à toutes les régions Régions AWS. Le

journal de suivi consigne les événements de toutes les Régions dans la partition AWS et livre les fichiers journaux dans le compartiment Amazon S3 de votre choix. En outre, vous pouvez configurer d'autres services AWS pour analyser plus en profondeur les données d'événement collectées dans les journaux CloudTrail et agir sur celles-ci.

Pour plus d'informations, consultez les rubriques suivantes dans le AWS CloudTrailGuide de l'utilisateur :

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

Toutes les actions AWS CodeConnections sont consignées par CloudTrail et documentées dans la Référence des API AWS CodeConnections. À titre d'exemple, les appels vers les actions `CreateConnection`, `DeleteConnection` et `GetConnection` génèrent des entrées dans les fichiers journaux CloudTrail.

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

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

Pour plus d'informations, consultez l'élément userIdentity CloudTrail.

Présentation des entrées des fichiers journaux

Un journal d'activité est une configuration qui permet la livraison d'événements sous forme de fichiers journaux vers un compartiment Amazon S3 que vous spécifiez. Les fichiers journaux CloudTrail peuvent contenir une ou plusieurs entrées. Un événement représente une demande individuelle émise à partir d'une source quelconque et comprend des informations sur l'action demandée, la date et l'heure de l'action, les paramètres de la demande, etc. Les fichiers journaux CloudTrail ne

constituent pas une série ordonnée retraçant les appels d'API publiques. Ils ne suivent aucun ordre précis.

L'exemple suivant présente une entrée de journal CloudTrail qui illustre `CreateConnection` action.

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type":"IAMUser",
        "principalId":"AIDACKCEVSQ6C2EXAMPLE",
        "arn":"arn:aws:iam::123456789012:user/Mary_Major",
        "accountId":"123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName":"Mary_Major"
    },
    "eventTime": "2020-04-21T01:09:48Z",
    "eventSource": "codestar-connections.amazonaws.com",
    "eventName": "CreateConnection",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "IP",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
 like Gecko) Chrome/80.0.3987.163 Safari/537.36",
    "requestParameters": {
        "providerType": "Bitbucket",
        "connectionName": "my-connection"
    },
    "responseElements": {
        "connectionArn": "arn:aws:codestar-connections:us-
west-2:123456789012:connection/7EXAMPLE-5da1-4867-960c-4918175ea3ce"
    },
    "requestID": "ac1fbc15-a84f-4568-9f90-f05f1a57749c",
    "eventID": "7548f5b0-7ecf-430f-84bf-72e364644359",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "recipientAccountId": "123456789012"
}
```

AWS CodeStar Connections et points de terminaison de VPC d'interface (AWS PrivateLink)

Vous pouvez établir une connexion privée entre votre VPC et AWS CodeStar Connections en créant un point de terminaison de VPC d'interface. Les points de terminaison d'interface sont

alimentés par AWS PrivateLink, une technologie qui vous permet d'accéder en privé aux API AWS CodeStar Connections sans passerelle Internet, périphérique NAT, connexion VPN ou connexion AWS Direct Connect. Les instances de votre VPC n'ont pas besoin d'adresses IP publiques pour communiquer avec les API AWS CodeStar Connections, car le trafic entre votre VPC et AWS CodeStar Connections ne quitte pas le réseau Amazon.

Chaque point de terminaison d'interface est représenté par une ou plusieurs interfaces réseau Elastic dans vos sous-réseaux.

Pour de plus amples informations, veuillez consulter Points de terminaison d'un VPC d'interface (AWS PrivateLink) dans le Guide de l'utilisateur Amazon VPC.

Considérations relatives aux points de terminaison de VPC AWS CodeStar Connections

Avant de configurer un point de terminaison de VPC d'interface pour AWS CodeStar Connections, assurez-vous de vérifier les point de terminaison d'interface dans le guide de l'utilisateur Amazon VPC.

AWS CodeStar Connections prend en charge l'exécution d'appels en direction de toutes ses actions d'API depuis votre VPC.

Les points de terminaison de VPC sont pris en charge dans toutes les régions AWS CodeStar Connections.

Concepts des points de terminaison d'un VPC

Les concepts clés liés aux points de terminaison d'un VPC sont les suivants :

Point de terminaison d'un VPC

Le point d'entrée de votre VPC qui vous permet de vous connecter par réseau privé à un service. Voici les différents types de points de terminaison d'un VPC. Créez le type de point de terminaison d'un VPC requis par le service pris en charge.

- Points de terminaison d'un VPC pour les actions AWS CodeStar Connections
- Points de terminaison d'un VPC pour les webhooks AWS CodeStar Connections

AWS PrivateLink

Une technologie qui fournit une connectivité réseau privé entre les VPC et les services.

Points de terminaison d'un VPC pour les actions AWS CodeStar Connections

Vous pouvez gérer les points de terminaison d'un VPC pour le service AWS CodeStar Connections.

Création de points de terminaison d'un VPC d'interface pour les actions AWS CodeStar Connections

Vous pouvez créer un point de terminaison de VPC pour le service AWS CodeStar Connections à l'aide de la console Amazon VPC ou de la AWS Command Line Interface (AWS CLI). Pour de plus amples informations, veuillez consulter Création d'un point de terminaison d'interface dans le Guide de l'utilisateur Amazon VPC.

Pour commencer à utiliser des connexions avec votre VPC, créez un point de terminaison de VPC d'interface pour AWS CodeStar Connections. Lorsque vous créez un point de terminaison de VPC pour AWS CodeStar Connections, choisissez AWS Services (Services AWS), et dans Service Name (Nom du service), choisissez :

- com.amazonaws.***region***.codestar-connections.api : cette option crée un point de terminaison de VPC pour les opérations de l'API AWS CodeStar Connections. Par exemple, choisissez cette option si vos utilisateurs utilisent la CLI AWS, l'API AWS CodeStar Connections ou les kits SDK AWS pour interagir avec AWS CodeStar Connections pour des opérations telles que `CreateConnection`, `ListConnections` et `CreateHost`.

Pour l'option Enable DNS name (Activer le nom DNS), si vous sélectionnez le DNS privé pour le point de terminaison, vous pouvez faire des demandes d'API à AWS CodeStar Connections en utilisant son nom DNS par défaut pour la région, par exemple `codestar-connections.us-east-1.amazonaws.com`.

> **Important**
>
> Le DNS privé est activé par défaut pour les points de terminaison créés pour des services AWS et des services partenaires AWS Marketplace.

Pour plus d'informations, consultez Accès à un service via un point de terminaison d'interface dans le Guide de l'utilisateur Amazon VPC.

Création d'une stratégie de points de terminaison de VPC pour les actions AWS CodeStar Connections

Vous pouvez attacher une stratégie de points de terminaison à votre point de terminaison d'un VPC qui contrôle l'accès à AWS CodeStar Connections. La politique spécifie les informations suivantes :

- Le principal qui peut exécuter des actions.
- Les actions qui peuvent être effectuées.
- Les ressources sur lesquelles les actions peuvent être exécutées.

Pour plus d'informations, consultez Contrôle de l'accès aux services avec points de terminaison d'un VPC dans le Guide de l'utilisateur Amazon VPC.

> **Note**
>
> Le point de terminaison com.amazonaws.*region*.codestar-connections.webhooks ne prend pas en charge les stratégies.

Exemple : stratégie de points de terminaison de VPC pour les actions AWS CodeStar Connections

Voici un exemple de stratégie de points de terminaison pour AWS CodeStar Connections. Lorsqu'elle est attachée à un point de terminaison, cette stratégie accorde l'accès aux actions AWS CodeStar Connections répertoriées pour tous les mandataires sur toutes les ressources.

```
{
  "Statement": [
    {
      "Sid": "GetConnectionOnly",
      "Principal": "*",
      "Action": [
        "codestar-connections:GetConnection"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

Points de terminaison d'un VPC pour les webhooks AWS CodeStar Connections

AWS CodeStar Connections crée des points de terminaison webhook pour vous lorsque vous créez ou supprimez un hôte avec une configuration VPC. Le nom du point de terminaison est com.amazonaws.***region***.codestar-connections.webhooks.

Avec le point de terminaison de VPC pour les webhooks GitHub, les hôtes peuvent envoyer des données d'événement via webhooks à vos services AWS intégrés sur le réseau Amazon.

> **Important**
>
> Lorsque vous configurez votre hôte pour GitHub Enterprise Server, AWS CodeStar Connections crée un point de terminaison de VPC pour les données d'événement webhooks. Si vous avez créé votre hôte avant le 24 novembre 2020 et que vous souhaitez utiliser les points de terminaison de VPC webhook PrivateLink, vous devez d'abord supprimer votre hôte, puis créer un nouvel hôte.

AWS CodeStar Connections gère le cycle de vie de ces points de terminaison. Pour supprimer le point de terminaison, vous devez supprimer la ressource hôte correspondante.

Utilisation des points de terminaison d'un VPC pour les hôtes AWS CodeStar Connections

Le point de terminaison webhook est l'endroit où les webhooks provenant de référentiels tiers sont envoyés pour le traitement de AWS CodeStar Connections. Un webhook décrit une action client. Lorsque vous effectuez un `git push`, le point de terminaison webhook reçoit un webhook du fournisseur détaillant le push. Par exemple, AWS CodeStar Connections peut demander à CodePipeline de démarrer votre pipeline.

Pour les fournisseurs de cloud, tels que Bitbucket, ou les hôtes GitHub Enterprise Server qui n'utilisent pas de VPC, le point de terminaison webhook VPC ne s'applique pas, car les fournisseurs envoient des webhooks à AWS CodeStar Connections où le réseau Amazon n'est pas utilisé.

Dépannage des problèmes de connexion

Les informations suivantes vous aident à résoudre les problèmes courants que vous êtes susceptible de rencontrer avec les connexions aux ressources dans AWS CodeBuild, AWS CodeDeploy et AWS CodePipeline.

Rubriques

Je ne peux pas créer de connexions

Vous ne disposez peut-être pas des autorisations suffisantes pour créer une connexion. Pour de plus amples informations, veuillez consulter Autorisations et exemples pour AWS CodeConnections.

Je reçois une erreur d'autorisation lorsque j'essaie de créer ou d'établir une connexion

Le message d'erreur suivant peut être renvoyé lorsque vous essayez de créer ou d'afficher une connexion dans la console CodePipeline.

Utilisateur : *`username`* n'est pas autorisé à exécuter : *`autorisation`* sur la ressource : *`connection-ARN`*

Si ce message s'affiche, assurez-vous de disposer des autorisations suffisantes.

Les autorisations permettant de créer et d'afficher des connexions dans la AWS Command Line Interface (AWS CLI) ou la AWS Management Console ne sont qu'une partie des autorisations dont vous avez besoin pour créer et établir des connexions sur la console. Les autorisations requises pour simplement afficher, modifier ou créer une connexion puis établir la connexion en attente doivent être limitées pour les utilisateurs qui n'ont besoin que de certaines tâches. Pour de plus amples informations, veuillez consulter Autorisations et exemples pour AWS CodeConnections.

Je reçois une erreur d'autorisation lorsque j'essaie d'utiliser une connexion

Le ou les messages d'erreur suivants peuvent être renvoyés si vous essayez d'utiliser une connexion dans la console CodePipeline, même si vous disposez des autorisations nécessaires pour répertorier, obtenir et créer des autorisations.

Vous n'avez pas réussi à authentifier votre compte.

Utilisateur : *username* n'est pas autorisé à exécuter : codestar-connections:UseConnection sur la ressource : *connection-ARN*

Si cela se produit, assurez-vous de disposer des autorisations suffisantes.

Assurez-vous de disposer des autorisations nécessaires à l'utilisation d'une connexion, y compris la liste des référentiels disponibles dans l'emplacement du fournisseur. Pour de plus amples informations, veuillez consulter Autorisations et exemples pour AWS CodeConnections.

La connexion n'est pas disponible ou n'est plus en attente

Si la console affiche un message indiquant qu'une connexion n'est pas disponible, sélectionnez Complete connection (Établir la connexion).

Si vous choisissez d'établir la connexion et qu'un message s'affiche indiquant que la connexion n'est pas en attente, vous pouvez annuler la demande, car la connexion est déjà disponible.

Ajouter des autorisations GitClone pour les connexions

Lorsque vous utilisez une connexion AWS CodeStar dans une action source et une action CodeBuild, l'artefact d'entrée peut être transmis à la génération de deux manières différentes :

- Par défaut : l'action source génère un fichier zip contenant le code que CodeBuild télécharge.
- Clone Git : le code source peut être téléchargé directement dans l'environnement de génération.

Le mode Clone Git vous permet d'interagir avec le code source en tant que référentiel Git fonctionnel. Pour utiliser ce mode, vous devez accorder à votre environnement CodeBuild les autorisations d'utilisation de la connexion.

Pour ajouter des autorisations à votre stratégie de rôle de service CodeBuild, vous créez une stratégie gérée par le client que vous attachez à votre rôle de service CodeBuild. Les étapes suivantes créent une stratégie dans laquelle l'autorisation `UseConnection` est spécifiée dans le champ `action` et l'Amazon Resource Name (ARN) de connexion est spécifié dans le champ `Resource`.

Pour utiliser la console pour ajouter les autorisations UseConnection

1. Pour trouver l'ARN de connexion de votre pipeline, ouvrez votre pipeline et cliquez sur l'icône (i) de votre action source. Le volet Configuration s'ouvre et l'ARN de connexion apparaît en regard de ConnectionArn. Vous ajoutez l'ARN de connexion à votre stratégie de rôle de service CodeBuild.
2. Pour trouver votre rôle de service CodeBuild, ouvrez le projet de génération utilisé dans votre pipeline et accédez à l'onglet Build details (Détails de génération).
3. Dans la section Environnement, choisissez le lien Service role (Rôle de service). Cela ouvre la AWS Identity and Access Management (IAM) où vous pouvez ajouter une nouvelle stratégie qui accorde l'accès à votre connexion.
4. Dans la console IAM, choisissez Attach policies (Attacher des stratégies), puis Créer une stratégie.

   Utilisez l'exemple de modèle de stratégie suivant. Ajoutez votre ARN de connexion dans le champ `Resource`, comme illustré dans cet exemple.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "codestar-connections:UseConnection",
            "Resource": "insert connection ARN here"
        }
    ]
}
```

Sous l'onglet JSON, collez votre stratégie.

5. Choisissez Review policy (Examiner une politique). Entrez un nom pour la stratégie (par exemple, **`connection-permissions`**), puis choisissez Créer une stratégie.
6. Revenez à la page Attach Permissions (Attacher des autorisations du rôle de service, actualisez la liste des stratégies et sélectionnez la stratégie que vous venez de créer. Sélectionnez Attach Policies (Attacher des politiques).

L'hôte n'est pas disponible

Si la console affiche un message indiquant qu'un hôte ne présente pas l'état `Available`, choisissez Set up host (Configurer l'hôte).

Suite à la première étape de la création de l'hôte, l'hôte créé présente l'état `Pending`. Pour déplacer l'hôte vers un état `Available`, vous devez choisir de configurer l'hôte dans la console. Pour de plus amples informations, veuillez consulter Configurer un hôte en attente.

> **Note**
>
> Vous ne pouvez pas utiliser la CLI AWS pour configurer un hôte `Pending`.

Résolution des problèmes liés à un hôte avec des erreurs de connexion

Les connexions et les hôtes peuvent passer à l'état d'erreur si l'application GitHub sous-jacente est supprimée ou modifiée. Les hôtes et les connexions à l'état d'erreur ne peuvent pas être restaurés et l'hôte doit être recréé.

- Des actions telles que la modification de la clé pem de l'application, la modification du nom de l'application (après la création initiale) entraîneront l'état d'erreur de l'hôte et de toutes les connexions associées.

Si la console ou la CLI renvoie un hôte ou une connexion liée à un hôte avec un état `Error`, vous pourriez avoir besoin de suivre l'étape suivante :

- Supprimez et recréez la ressource hôte, puis réinstallez l'application d'enregistrement de l'hôte. Pour de plus amples informations, veuillez consulter Création d'un hôte.

Je ne suis pas en mesure de créer une connexion pour mon hôte

Pour créer une connexion ou un hôte, les conditions suivantes sont requises.

- Votre hôte doit présenter l'état DISPONIBLE. Pour plus d'informations, consultez
- Les connexions doivent être créées dans la même région que l'hôte.

Résolution des problèmes liés à la configuration d'un VPC pour votre hôte

Lorsque vous créez une ressource hôte, vous devez fournir des informations de connexion réseau ou de VPC pour l'infrastructure sur laquelle votre instance GitHub Enterprise Server est installée. Pour résoudre les problèmes liés à la configuration de votre VPC ou sous-réseau pour votre hôte, utilisez l'exemple d'informations sur les VPC illustré ici comme référence.

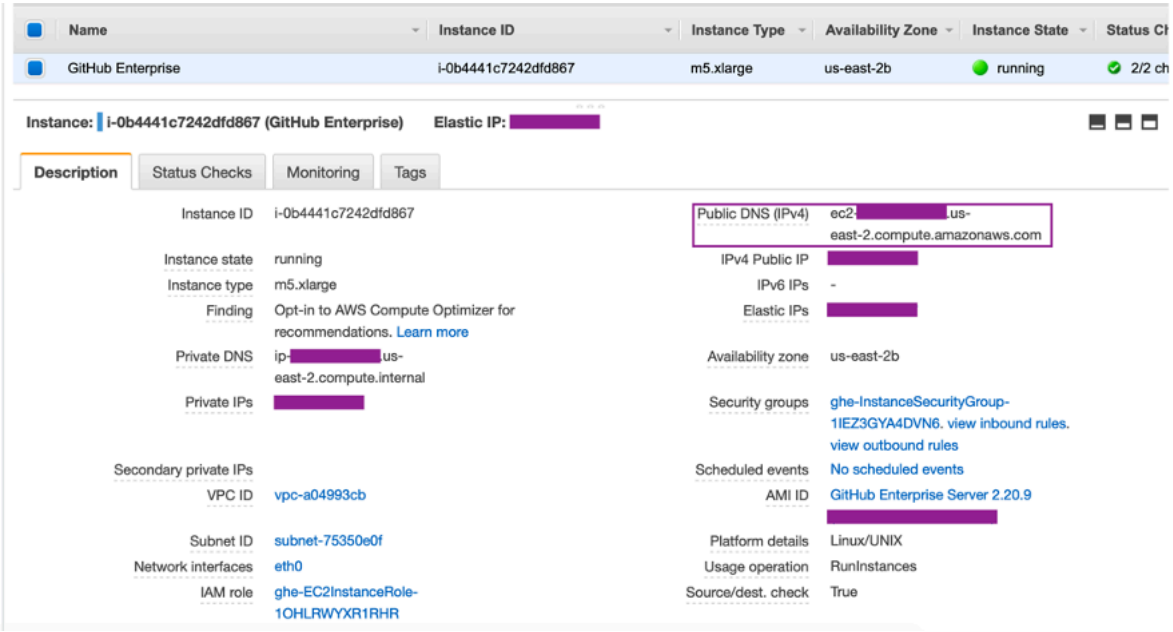
> **Note**
>
> Utilisez cette section pour résoudre les problèmes liés à votre configuration d'hôte GitHub Enterprise Server au sein d'un VPC Amazon. Pour la résolution des problèmes liés à votre connexion configurée pour utiliser le point de terminaison webhook pour VPC (PrivateLink), consultez Résolution des problèmes liés aux points de terminaison de VPC webhook (PrivateLink) pour les connexions GitHub Enterprise Server.

Dans cet exemple, vous devez utiliser le processus suivant pour configurer le VPC et le serveur sur lesquels votre instance GitHub Enterprise Server sera installée :

1. Créez un VPC. Pour de plus amples informations, veuillez consulter https://docs.aws.amazon.com/vpc/latest/userguide/working-with-vpcs.html#Create-VPC.
2. Créer un sous-réseau dans votre VPC Pour de plus amples informations, veuillez consulter https://docs.aws.amazon.com/vpc/latest/userguide/working-with-vpcs.html#AddaSubnet.
3. Lancez une instance dans votre VPC Pour de plus amples informations, veuillez consulter https://docs.aws.amazon.com/vpc/latest/userguide/working-with-vpcs.html#VPC_Launch_Instance.

> **Note**
>
> Chaque VPC peut être associé à un seul hôte (instance GitHub Enterprise Server) à la fois.

L'image suivante montre une instance EC2 lancée à l'aide de l'AMI GitHub Enterprise.



Lorsque vous utilisez un VPC pour une connexion GitHub Enterprise Server, vous devez fournir les éléments suivants pour votre infrastructure lorsque vous configurez votre hôte :

- ID de VPC : le VPC du serveur sur lequel votre instance GitHub Enterprise Server est installée ou un VPC qui a accès à votre instance GitHub Enterprise Server installée via VPN ou Direct Connect.
- Un ou plusieurs ID de sous-réseau : le sous-réseau du serveur sur lequel votre instance GitHub Enterprise Server est installée ou un sous-réseau qui a accès à votre instance GitHub Enterprise Server installée via VPN ou Direct Connect.
- Un ou plusieurs groupes de sécurité : le groupe de sécurité du serveur sur lequel votre instance GitHub Enterprise Server est installée ou un groupe de sécurité qui a accès à votre instance GitHub Enterprise Server installée via VPN ou Direct Connect.
- Point de terminaison : préparez votre point de terminaison de serveur et passez à l'étape suivante.

Pour plus d'informations sur l'utilisation des VPC et des sous-réseaux, veuillez consulter Dimensionnement des VPC et des sous-réseaux pour IPv4 dans le guide de l'utilisateur Amazon VPC.

Rubriques

- Je ne parviens pas à obtenir un hôte à l'état en attente
- Je ne parviens pas à obtenir un hôte à l'état disponible

- Ma connexion/mon hôte fonctionnait, puis a cessé de fonctionner
- Je ne suis pas en mesure de supprimer mes interfaces réseau

Je ne parviens pas à obtenir un hôte à l'état en attente

Si votre hôte passe à l'état VPC_CONFIG_FAILED_INITIALIZATION, cela est probablement dû à un problème avec le VPC, les sous-réseaux ou les groupes de sécurité que vous avez sélectionnés pour votre hôte.

- Le VPC, les sous-réseaux et les groupes de sécurité doivent tous appartenir au compte créant l'hôte.
- Les sous-réseaux et groupes de sécurité doivent appartenir au VPC sélectionné.
- Chaque sous-réseaux fournit doit se trouver dans deux zones de disponibilité différentes.
- L'utilisateur qui crée l'hôte doit disposer des autorisations IAM suivantes :

```
ec2:CreateNetworkInterface
ec2:CreateTags
ec2:DescribeDhcpOptionsec2:DescribeNetworkInterfaces
ec2:DescribeSubnets
ec2:DeleteNetworkInterface
ec2:DescribeVpcs
ec2:CreateVpcEndpoint
ec2:DeleteVpcEndpoints
ec2:DescribeVpcEndpoints
```

Je ne parviens pas à obtenir un hôte à l'état disponible

Si vous ne parvenez pas à terminer la configuration de l'application AWS CodeStar Connections pour votre hôte, cela peut être dû à un problème avec vos configurations VPC ou votre instance GitHub Enterprise Server.

- Si vous n'utilisez pas d'autorité de certification publique, vous devrez fournir à votre hôte un certificat TLS qui est utilisé par votre instance GitHub Enterprise. La valeur du certificat TLS doit être la clé publique du certificat.
- Vous devez être administrateur de l'instance GitHub Enterprise Server pour créer des applications GitHub.

Ma connexion/mon hôte fonctionnait, puis a cessé de fonctionner

Si une connexion/un hôte fonctionnait auparavant et ne fonctionne plus, cela peut être dû à un changement de configuration dans votre VPC ou l'application GitHub a été modifiée. Vérifiez les éléments suivants :

- Le groupe de sécurité attaché à la ressource hôte que vous avez créée pour votre connexion a maintenant changé ou n'a plus accès au serveur GitHub Enterprise. AWS CodeStar Connections nécessite un groupe de sécurité doté d'une connectivité à l'instance de GitHub Enterprise Server.
- L'adresse IP du serveur DNS a récemment changé. Vous pouvez vérifier cela en vérifiant les options DHCP attachées au VPC spécifié dans la ressource hôte que vous avez créée pour votre connexion. Notez que si vous êtes récemment passé d'AmazonProvidedDNS à un serveur DNS personnalisé ou si vous avez commencé à utiliser un nouveau serveur DNS personnalisé, l'hôte/la connexion cessera de fonctionner. Pour résoudre ce problème, supprimez votre hôte existant et recréez-le, ce qui stockerait les derniers paramètres DNS dans notre base de données.
- Les paramètres des ACL réseau ont changé et n'autorisent plus les connexions HTTP au sous-réseau où se trouve votre infrastructure GitHub Enterprise Server.
- Toutes les configurations de l'application AWS CodeStar Connections sur votre GitHub Enterprise Server ont été modifiées. Les modifications apportées à l'une des configurations, notamment les URL ou les secrets d'application, peuvent rompre la connectivité entre votre instance GitHub Enterprise Server installée et AWS CodeStar Connections.

Je ne suis pas en mesure de supprimer mes interfaces réseau

Si vous ne parvenez pas à détecter vos interfaces réseau, vérifiez les points suivants :

- Les interfaces réseau créées par AWS CodeStar Connections ne peuvent être supprimées qu'en supprimant l'hôte. Elles ne peuvent pas être supprimées manuellement par l'utilisateur.
- Vous devez détenir les autorisations suivants :

```
ec2:DescribeNetworkInterfaces
ec2:DeleteNetworkInterface
```

Résolution des problèmes liés aux points de terminaison de VPC webhook (PrivateLink) pour les connexions GitHub Enterprise Server

Lorsque vous créez un hôte avec une configuration VPC, le point de terminaison VPC webhook est créé pour vous.

> **Note**
>
> Utilisez cette section pour la résolution des problèmes liés à votre connexion configurée pour utiliser le point de terminaison webhook pour VPC (PrivateLink). Pour résoudre les problèmes liés à votre configuration d'hôte GitHub Enterprise Server au sein d'un VPC Amazon, consultez Résolution des problèmes liés à la configuration d'un VPC pour votre hôte.

Lorsque vous créez une connexion à un type de fournisseur installé et que vous avez spécifié que votre serveur était configuré au sein d'un VPC, AWS CodeStar Connections crée votre hôte et le point de terminaison de VPC (PrivateLink) pour les webhooks est créé pour vous. Cela permet à l'hôte d'envoyer des données d'événement via webhooks à vos services AWS intégrés sur le réseau Amazon. Pour de plus amples informations, veuillez consulter AWS CodeStar Connections et points de terminaison de VPC d'interface (AWS PrivateLink).

Rubriques

- Je ne suis pas en mesure de supprimer mes points de terminaison de VPC webhook

Je ne suis pas en mesure de supprimer mes points de terminaison de VPC webhook

AWS CodeStar Connections gère le cycle de vie de ces points de terminaison de VPC webhook pour votre hôte. Si vous souhaitez supprimer le point de terminaison, vous devez supprimer la ressource hôte correspondante.

- Les points de terminaison de VPC webhook créés par AWS CodeStar Connections ne peuvent être supprimés qu'en supprimant l'hôte. Ils ne peuvent pas être supprimés manuellement.
- Vous devez détenir les autorisations suivants :

```
ec2:DescribeNetworkInterfaces
ec2:DeleteNetworkInterface
```

Résolution des problèmes liés à un hôte créé avant le 24 novembre 2020

Depuis le 24 novembre 2020, lorsque AWS CodeStar Connections configure votre hôte, une prise en charge de point de terminaison de VPC (PrivateLink) supplémentaire est configurée pour vous. Pour les hôtes créés avant cette mise à jour, utilisez cette section de résolution des problèmes.

Pour de plus amples informations, veuillez consulter AWS CodeStar Connections et points de terminaison de VPC d'interface (AWS PrivateLink).

Rubriques

- J'ai un hôte qui a été créé avant le 24 novembre 2020 et je veux utiliser les points de terminaison de VPC (PrivateLink) pour les webhooks
- Je ne parviens pas à obtenir un hôte à l'état disponible (erreur de VPC)

J'ai un hôte qui a été créé avant le 24 novembre 2020 et je veux utiliser les points de terminaison de VPC (PrivateLink) pour les webhooks

Lorsque vous configurez votre hôte pour GitHub Enterprise Server, le point de terminaison de VPC webhook est créé pour vous. Les connexions utilisent désormais les points de terminaison de VPC webhook PrivateLink. Si vous avez créé votre hôte avant le 24 novembre 2020 et que vous souhaitez utiliser les points de terminaison de VPC webhook PrivateLink, vous devez d'abord supprimer votre hôte, puis créer un nouvel hôte.

Je ne parviens pas à obtenir un hôte à l'état disponible (erreur de VPC)

Si votre hôte a été créé avant le 24 novembre 2020 et que vous ne parvenez pas à terminer la configuration de l'application AWS CodeStar Connections pour votre hôte, cela peut être dû à un problème avec vos configurations VPC ou votre instance GitHub Enterprise Server.

Votre VPC aura besoin d'une passerelle NAT (ou d'un accès Internet sortant) afin que votre instance GitHub Enterprise Server puisse envoyer du trafic réseau sortant pour les webhooks GitHub.

Impossible de créer la connexion pour un référentiel GitHub

Problème :

Étant donné qu'une connexion à un référentiel GitHub utilise AWS Connector for GitHub, vous avez besoin des autorisations du propriétaire de l'organisation ou des autorisations d'administrateur sur le référentiel pour créer la connexion.

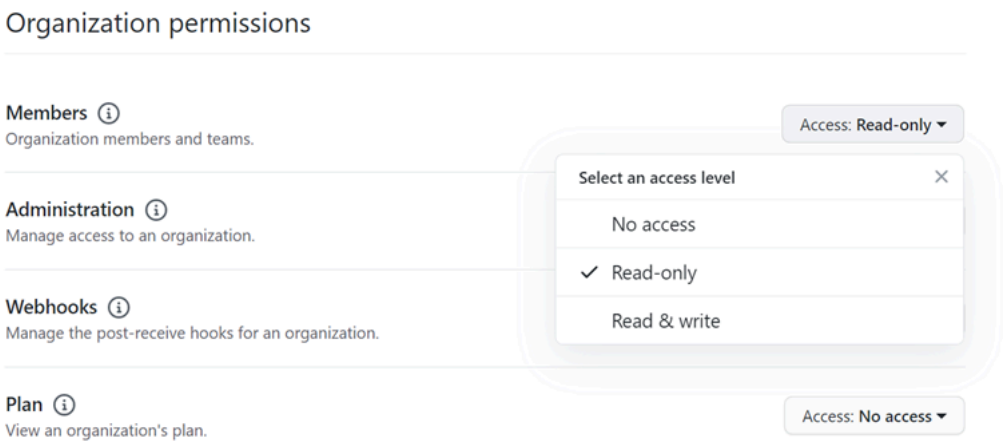
Correctifs possibles : pour plus d'informations sur les niveaux d'autorisation pour un référentiel GitHub, consultez https://docs.github.com/en/free-pro-team@latest/github/setting-up-and-managing-organizations-and-teams/permission-levels-for-an-organization.

Modifiez les autorisations de l'application de connexion GitHub Enterprise Server

Si vous avez installé l'application pour GitHub Enterprise Server au plus tard le 23 décembre 2020, vous devrez peut-être accorder aux membres de l'organisation un accès en lecture seule à l'application. Si vous êtes le propriétaire de l'application GitHub, procédez comme suit pour modifier les autorisations de l'application installée lors de la création de votre hôte.

> **Note**
>
> Vous devez suivre ces étapes sur votre instance GitHub Enterprise Server et vous devez être le propriétaire de l'application GitHub.

1. Dans GitHub, depuis la liste déroulante d'options sur votre photo de profil, choisissez Settings (Paramètres).
2. Choisissez Developer settings (Paramètres du développeur), puis GitHub Apps (Applications GitHub).
3. Dans la liste des applications, choisissez le nom de l'application pour votre connexion, puis choisissez Permissions and events (Autorisations et événements) dans l'affichage des paramètres.
4. Sous Organization permissions (Autorisations d'organisation), pour Members (Membres), choisissez Read-only (Lecture seule) à partir de la liste déroulante Access (Accès).



5. Dans Add a note to users (Ajouter une note aux utilisateurs), ajoutez une description de la raison de la mise à jour. Sélectionnez Save Changes (Enregistrer les modifications).

Erreur de connexion lors de la connexion à GitHub : « Un problème est survenu, assurez-vous que les cookies sont activés dans votre navigateur » ou « Le propriétaire d'une organisation doit installer l'application GitHub »

Problème :

Pour créer la connexion pour un référentiel GitHub, vous devez être le propriétaire de l'organisation GitHub. Pour les référentiels qui ne font pas partie d'une organisation, vous devez en être le propriétaire. Lorsqu'une connexion est créée par une personne autre que le propriétaire de l'organisation, une demande est créée pour le propriétaire de l'organisation et l'une des erreurs suivantes s'affiche :

Un problème est survenu, assurez-vous que les cookies sont activés dans votre navigateur

OU

Le propriétaire d'une organisation doit installer l'application GitHub

Correctifs possibles : pour les référentiels d'une organisation GitHub, le propriétaire de l'organisation doit créer la connexion au référentiel GitHub. Pour les référentiels qui ne font pas partie d'une organisation, vous devez en être le propriétaire.

Je souhaite augmenter mes limites de connexion

Vous pouvez demander une augmentation de limite pour certaines limites dans AWS CodeStar Connections. Pour de plus amples informations, veuillez consulter Quotas de connexions.

Quotas de connexions

Les tableaux suivants répertorient les quotas (également appelés limites) pour les connexions dans la console Outils pour développeurs.

Les quotas de ce tableau s'appliquent par Région AWS et peuvent être augmentés. Pour demander une augmentation, utilisez la console Support Center. Pour des informations sur la Région AWS et sur les quotas qui peuvent être modifiés, consultez Service Quotas AWS.

> **Note**
>
> Vous devez activer la Région AWS Europe (Milan) avant de pouvoir l'utiliser. Pour plus d'informations, consultez Activer une région.

Ressource	Limite par défaut
Nombre maximal de connexions par Compte AWS	250

Les quotas de ce tableau sont fixes et ne peuvent pas être modifiés.

Ressource	Limite par défaut
Nombre maximal de caractères dans les noms de connexion	32 caractères
Nombre maximal d'hôtes par Compte AWS	50
Nombre maximal de liens de référentiel	100
Nombre maximal de configurations de synchronisation de la pile AWS CloudFormation	100
Nombre maximal de configurations de synchronisation par lien de référentiel	100
Nombre maximal de configurations de synchronisation par branche	50

Adresses IP à ajouter à votre liste d'autorisation

Si vous implémentez le filtrage IP ou si vous autorisez certaines adresses IP sur les instances Amazon EC2, ajoutez les adresses IP suivantes à votre liste d'autorisations. Cela permet de se connecter à des fournisseurs tels que GitHub Bitbucket.

La table suivante répertorie les adresses IP pour les connexions dans la console Outils pour développeurs par Région AWS.

> **Note**
>
> Pour la région Europe (Milan), vous devez activer cette région avant de pouvoir l'utiliser. Pour plus d'informations, consultez Activer une région.

Région	Adresses IP
USA Ouest (Oregon) (us-west-2)	35,160,210,199, 54,71,206,108, 54,71,36,205
USA Est (Virginie du Nord) (us-east-1)	3,216,216,90, 3,216,243,220, 3,217,241,85
Europe (Irlande) (eu-west-1)	34,242,64,82, 52,18,37,201, 54,77,75,62
USA Est (Ohio) (us-east-2)	18,217,188,190, 18,218,158,91, 18,220,4,80
Asie-Pacifique (Singapour) (ap-southeast-1)	18,138,171,151, 18,139,22,70, 3,1157,176
Asie-Pacifique (Sydney) (ap-southeast-2)	13,236,59,253, 52,64,166,86, 54,206,1112
Asie-Pacifique (Tokyo) (ap-northeast-1)	52,2196.132,231, 54,95,1333,227, 181,13,91
Europe (Francfort) (eu-central-1)	18,146,145,164, 3,121,252,59, 52,59,14,195
Asie-Pacifique (Séoul) (ap-northeast-2)	13,125,8239, 13,209,223,177, 3,37,200,23
Asie-Pacifique (Mumbai) (ap-south-1)	13,234,199,152, 13,235,29,220, 35,154,23 0,124
Amérique du Sud (São Paulo) (sa-east-1)	18,229,77,26, 54,233,226,52, 54,233,207,69
Canada (Centre) (ca-central-1)	15,222,219,210, 35,182,166,138, 99,79,111 ,198
Europe (Londres) (eu-west-2)	3,9,97,205, 35,177,150,185, 35,177,200,225
US Ouest (N. California) (us-west-1)	52,52,16.175, 52,8,63,87

Région	Adresses IP
Europe (Paris) (eu-west-3)	35,181,127,138, 35,181,145,22, 35,181,20,200
Europe (Stockholm) (eu-north-1)	13,48,66,148, 13,488,8,79, 13,53,78,182
Europe (Milan) (eu-south-1)	18,102,28,105, 18,102,35,130, 18,102,8,116

Sécurité pour les fonctions de la console Outils pour développeurs

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

La sécurité est une responsabilité partagée entre vous AWS et vous. Le modèle de responsabilité partagée décrit cette notion par les termes sécurité du cloud et sécurité dans le cloud :

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

Cette documentation vous aide à comprendre comment appliquer le modèle de responsabilité partagée lors de l'utilisation AWS CodeStar des notifications et des AWS CodeStar connexions. Les rubriques suivantes expliquent comment configurer les AWS CodeStar notifications et les AWS CodeStar connexions pour atteindre vos objectifs de sécurité et de conformité. Vous apprendrez également à utiliser d'autres AWS services qui vous aident à surveiller et à sécuriser vos ressources de AWS CodeStar notifications et de AWS CodeStar connexions.

Pour plus d'informations sur la sécurité des services de la console Outils pour développeurs, consultez ce qui suit :

- CodeBuild Sécurité
- CodeCommit Sécurité
- CodeDeploy Sécurité
- CodePipeline Sécurité

Présentation du contenu des notifications et de la sécurité

Les notifications fournissent des informations sur les ressources aux utilisateurs abonnés aux cibles de règle de notification que vous configurez. Cela peut inclure des informations sur les ressources de vos outils de développement, notamment le contenu de référentiel, les statuts de génération et de déploiement, et les exécutions de pipeline.

Par exemple, vous pouvez configurer une règle de notification pour un référentiel CodeCommit afin d'inclure des commentaires sur les validations ou les pull requests. Dans ce cas, les notifications envoyées en réponse à cette règle peuvent contenir la ou les lignes de code référencées dans ces commentaires. De même, vous pouvez configurer une règle de notification pour un projet de construction CodeBuild afin d'inclure les réussites ou les échecs pour les états et les phases de construction. Les notifications envoyées en réponse à cette règle contiendront ces informations.

Vous pouvez configurer une règle de notification pour un pipeline CodePipeline afin d'inclure des informations sur les approbations manuelles, et les notifications envoyées en réponse à cette règle peuvent contenir le nom de la personne fournissant cette approbation. Vous pouvez configurer une règle de notification pour une application CodeDeploy afin d'indiquer le succès du déploiement, et les notifications envoyées en réponse à cette règle peuvent contenir des informations sur la cible de déploiement.

Les notifications peuvent inclurent des informations spécifiques au projet, telles que les statuts de génération et de déploiement, les lignes de code contenant des commentaires et les approbations de pipeline. Afin de garantir la sécurité de votre projet, veillez à vérifier régulièrement les cibles des règles de notification, ainsi que la liste des abonnés des rubriques Amazon SNS spécifiées comme cibles. De plus, le contenu des notifications envoyées en réponse aux événements peut changer au fur et à mesure que des fonctionnalités supplémentaires sont ajoutées aux services sous-jacents. Cette modification peut être appliquée sans préavis aux règles de notification déjà existantes. Pensez à vérifier régulièrement le contenu des messages de notification pour vous assurer que vous comprenez ce qui est envoyé, ainsi qu'à qui ce contenu est envoyé.

Pour plus d'informations sur les types d'événements disponibles pour les règles de notification, consultez Concepts de notification.

Vous pouvez choisir de limiter les détails inclus dans les notifications à ce qui est inclus dans un événement. C'est ce que l'on appelle le type de détail Basic (Élémentaire). Ces événements contiennent exactement les mêmes informations que celles envoyées à Amazon EventBridge et Amazon CloudWatch Events.

Les services de console Developer Tools, tels que CodeCommit, peuvent choisir d'ajouter des informations sur certains ou tous leurs types d'événements dans les messages de notification, au-delà de ce qui est disponible lors d'un événement. Ces renseignements supplémentaires pourraient être ajoutés à tout moment afin d'améliorer les types d'événements actuels ou de compléter les types d'événements futurs. Vous pouvez choisir d'inclure des informations supplémentaires sur l'événement, le cas échéant, dans la notification en choisissant le type de détail Full (Complet). Pour plus d'informations, voir Types de détails.

Protection des données dans AWS CodeStar Notifications et AWS CodeStar Connections

Le modèle de responsabilité partagée d'AWS s'applique à la protection des données dans AWS CodeStar Notifications et AWS CodeStar Connections. Comme décrit dans ce modèle, AWS est responsable de la protection de l'infrastructure globale sur laquelle l'ensemble d'AWS Cloud s'exécute. La gestion du contrôle de votre contenu hébergé sur cette infrastructure relève de votre responsabilité. Vous êtes également responsable des tâches de configuration et de gestion de la sécurité pour les Services AWS que vous utilisez. Pour en savoir plus sur la confidentialité des données, consultez Questions fréquentes (FAQ) sur la confidentialité des données. Pour en savoir plus sur la protection des données en Europe, consultez le billet de blog Modèle de responsabilité partagée AWSet RGPD (Règlement général sur la protection des données) sur le AWSBlog de sécurité.

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

- Utilisez l'authentification multifactorielle (MFA) avec chaque compte.
- Utilisez les certificats SSL/TLS pour communiquer avec les ressources AWS. Nous exigeons TLS 1.2 et recommandons TLS 1.3.
- Configurez une API (Interface de programmation) et le journal de l'activité des utilisateurs avec AWS CloudTrail.
- Utilisez des solutions de chiffrement AWS, ainsi que tous les contrôles de sécurité par défaut au sein des Services AWS.

- Utilisez des services de sécurité gérés avancés tels qu'Amazon Macie, qui contribuent à la découverte et à la sécurisation des données sensibles stockées dans Amazon S3.
- Si vous avez besoin de modules cryptographiques validés FIPS (Federal Information Processing Standard) 140-2 lorsque vous accédez à AWS via une CLI (Interface de ligne de commande) ou une API (Interface de programmation), utilisez un point de terminaison FIPS (Federal Information Processing Standard). Pour en savoir plus sur les points de terminaison FIPS (Federal Information Processing Standard) disponibles, consultez Federal Information Processing Standard (FIPS) 140-2 (Normes de traitement de l'information fédérale).

Nous vous recommandons fortement de ne jamais placer d'informations confidentielles ou sensibles, telles que les adresses e-mail de vos clients, dans des balises ou des champs de texte libre tels que le champ Name (Nom). Cela inclut l'utilisation de AWS CodeStar Notifications et AWS CodeStar Connections ou d'autres Services AWS à l'aide de la console, de l'API, de la AWS CLI ou des kits SDK AWS. Toutes les données que vous saisissez dans des balises ou des champs de texte de forme libre utilisés pour les noms peuvent être utilisées à des fins de facturation ou dans les journaux de diagnostic. Si vous fournissez une adresse URL à un serveur externe, nous vous recommandons fortement de ne pas inclure d'informations d'identification dans l'adresse URL permettant de valider votre demande adressée à ce serveur.

Gestion des identités et des accès pour les AWS CodeStar notifications et AWS CodeStar les connexions

AWS Identity and Access Management (IAM) est un outil Service AWS qui permet à un administrateur de contrôler en toute sécurité l'accès aux AWS ressources. Les administrateurs IAM contrôlent qui peut être authentifié (connecté) et autorisé (autorisé) à utiliser les ressources de AWS CodeStar notifications et de AWS CodeStar connexions. IAM est un Service AWS outil que vous pouvez utiliser sans frais supplémentaires.

Rubriques

- Exemples de politiques basées sur l'identité
- Utilisation de balises pour contrôler l'accès aux ressources AWS CodeStar Connections
- Utilisation de notifications et de connexions dans la console
- Autorisation accordée aux utilisateurs pour afficher leurs propres autorisations
- Résolution des problèmes liés aux AWS CodeStar notifications et aux AWS CodeStar connexions (identité et accès)
- Utilisation de rôles liés à un service pour AWS CodeStar Notifications
- Utilisation des rôles liés aux services pour AWS CodeConnections
- Politiques AWS gérées pour AWS CodeConnections

Public ciblé

La façon dont vous utilisez AWS Identity and Access Management (IAM) varie en fonction du travail que vous effectuez dans AWS CodeStar Notifications et AWS CodeStar connexions.

Utilisateur du service : si vous utilisez le service AWS CodeStar Notifications et AWS CodeStar connexions pour effectuer votre travail, votre administrateur vous fournit les informations d'identification et les autorisations dont vous avez besoin. Au fur et à mesure que vous utilisez davantage de fonctionnalités de AWS CodeStar notifications et de AWS CodeStar connexions pour effectuer votre travail, vous aurez peut-être besoin d'autorisations supplémentaires. En comprenant bien la gestion des accès, vous saurez demander les autorisations appropriées à votre administrateur. Si vous ne parvenez pas à accéder à une fonctionnalité dans AWS CodeStar Notifications et AWS CodeStar connexions, consultezRésolution des problèmes liés aux AWS CodeStar notifications et aux AWS CodeStar connexions (identité et accès).

Administrateur du service — Si vous êtes responsable des ressources de AWS CodeStar notifications et de AWS CodeStar connexions au sein de votre entreprise, vous avez probablement un accès complet aux AWS CodeStar notifications et aux AWS CodeStar connexions. Il vous incombe de déterminer à quelles fonctionnalités et ressources de AWS CodeStar notifications et de AWS CodeStar connexions les utilisateurs de vos services doivent accéder. Vous devez ensuite soumettre les demandes à votre administrateur IAM pour modifier les autorisations des utilisateurs de votre service. Consultez les informations sur cette page pour comprendre les concepts de base d'IAM. Pour en savoir plus sur la manière dont votre entreprise peut utiliser IAM avec AWS CodeStar les notifications et les AWS CodeStar connexions, consultezFonctionnement des fonctions de la console des outils pour développeurs avec IAM.

Administrateur IAM : si vous êtes administrateur IAM, vous souhaiterez peut-être en savoir plus sur la manière dont vous pouvez rédiger des politiques pour gérer l'accès aux AWS CodeStar notifications et AWS CodeStar aux connexions. Pour consulter AWS CodeStar des exemples de politiques basées sur l'identité relatives aux notifications et aux AWS CodeStar connexions que vous pouvez utiliser dans IAM, consultez. Exemples de politiques basées sur l'identité

Authentification par des identités

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

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

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

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

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

Utilisateur racine d'un compte AWS

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

Utilisateurs et groupes IAM

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

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

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

Rôles IAM

Un rôle IAM est une identité au sein de vous Compte AWS dotée d'autorisations spécifiques. Le concept ressemble à celui d'utilisateur IAM, mais le rôle IAM n'est pas associé à une personne en

particulier. Vous pouvez assumer temporairement un rôle IAM dans le en AWS Management Console changeant de rôle. Vous pouvez assumer un rôle en appelant une opération d' AWS API AWS CLI ou en utilisant une URL personnalisée. Pour plus d'informations sur les méthodes d'utilisation des rôles, consultez Utilisation de rôles IAM dans le Guide de l'utilisateur IAM.

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

- Accès utilisateur fédéré – Pour attribuer des autorisations à une identité fédérée, vous créez un rôle et définissez des autorisations pour le rôle. Quand une identité externe s'authentifie, l'identité est associée au rôle et reçoit les autorisations qui sont définies par celui-ci. Pour obtenir des informations sur les rôles pour la fédération, consultez Création d'un rôle pour un fournisseur d'identité tiers (fédération) dans le Guide de l'utilisateur IAM. Si vous utilisez IAM Identity Center, vous configurez un jeu d'autorisations. IAM Identity Center met en corrélation le jeu d'autorisations avec un rôle dans IAM afin de contrôler à quoi vos identités peuvent accéder après leur authentification. Pour plus d'informations sur les jeux d'autorisations, veuillez consulter la rubrique Jeux d'autorisations dans le Guide de l'utilisateur AWS IAM Identity Center .
- Autorisations d'utilisateur IAM temporaires : un rôle ou un utilisateur IAM peut endosser un rôle IAM pour profiter temporairement d'autorisations différentes pour une tâche spécifique.
- Accès intercompte : vous pouvez utiliser un rôle IAM pour permettre à un utilisateur (principal de confiance) d'un compte différent d'accéder aux ressources de votre compte. Les rôles constituent le principal moyen d'accorder l'accès intercompte. Toutefois, dans certains Services AWS cas, vous pouvez associer une politique directement à une ressource (au lieu d'utiliser un rôle comme proxy). Pour en savoir plus sur la différence entre les rôles et les politiques basées sur les ressources pour l'accès intercompte, consultez Différence entre les rôles IAM et les politiques basées sur les ressources dans le Guide de l'utilisateur IAM.
- Accès multiservices — Certains Services AWS utilisent des fonctionnalités dans d'autres Services AWS. Par exemple, lorsque vous effectuez un appel dans un service, il est courant que ce service exécute des applications dans Amazon EC2 ou stocke des objets dans Amazon S3. Un service peut le faire en utilisant les autorisations d'appel du principal, une fonction de service ou un rôle lié au service.
  - Sessions d'accès direct (FAS) : lorsque vous utilisez un utilisateur ou un rôle IAM pour effectuer des actions AWS, vous êtes considéré comme un mandant. Lorsque vous utilisez certains services, l'action que vous effectuez est susceptible de lancer une autre action dans un autre service. FAS utilise les autorisations du principal appelant et Service AWS, associées Service AWS à la demande, pour adresser des demandes aux services en aval. Les demandes FAS ne sont effectuées que lorsqu'un service reçoit une demande qui nécessite des interactions avec

d'autres personnes Services AWS ou des ressources pour être traitée. Dans ce cas, vous devez disposer d'autorisations nécessaires pour effectuer les deux actions. Pour plus de détails sur la politique relative à la transmission de demandes FAS, consultez Sessions de transmission d'accès.

- Fonction du service : il s'agit d'un rôle IAM attribué à un service afin de réaliser des actions en votre nom. Un administrateur IAM peut créer, modifier et supprimer une fonction du service à partir d'IAM. Pour plus d'informations, consultez Création d'un rôle pour la délégation d'autorisations à un Service AWS dans le Guide de l'utilisateur IAM.
- Rôle lié à un service — Un rôle lié à un service est un type de rôle de service lié à un. Service AWS Le service peut endosser le rôle afin d'effectuer une action en votre nom. Les rôles liés au service apparaissent dans votre Compte AWS fichier et appartiennent au service. Un administrateur IAM peut consulter, mais ne peut pas modifier, les autorisations concernant les rôles liés à un service.

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

Pour savoir dans quel cas utiliser des rôles ou des utilisateurs IAM, consultez Quand créer un rôle IAM (au lieu d'un utilisateur) dans le Guide de l'utilisateur IAM.

Gestion des accès à l'aide de politiques

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

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

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

Les politiques IAM définissent les autorisations d'une action, quelle que soit la méthode que vous utilisez pour exécuter l'opération. Par exemple, supposons que vous disposiez d'une politique qui autorise l'action `iam:GetRole`. Un utilisateur appliquant cette politique peut obtenir des informations sur le rôle à partir de AWS Management Console AWS CLI, de ou de l' AWS API.

Politiques basées sur l'identité

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

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

Fonctionnement des fonctions de la console des outils pour développeurs avec IAM

Avant d'utiliser IAM pour gérer l'accès aux fonctions de la console Outils pour développeurs, vous devez comprendre quelles sont les fonctions IAM disponibles. Pour obtenir une vue d'ensemble du fonctionnement des notifications et des autres AWS services avec IAM, consultez la section AWS Services compatibles avec IAM dans le Guide de l'utilisateur d'IAM.

Rubriques

- Stratégies basées sur l'identité dans la console Outils pour développeurs
- AWS CodeStar Politiques basées sur les ressources relatives aux notifications et aux AWS CodeStar connexions
- Autorisation basée sur les balises
- Rôles IAM

Stratégies basées sur l'identité dans la console Outils pour développeurs

Avec les politiques IAM basées sur l'identité, vous pouvez spécifier des actions et ressources autorisées ou refusées, ainsi que les conditions dans lesquelles les actions sont autorisées ou refusées. AWS CodeStar Les notifications et AWS CodeStar les connexions prennent en charge des actions, des ressources et des clés de condition spécifiques. Pour en savoir plus sur tous les éléments que vous utilisez dans une politique JSON, consultez Références des éléments de politique JSON IAM dans le Guide de l'utilisateur IAM.

Actions

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

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

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

Les actions de stratégie pour les notifications dans la console Outils pour développeurs utilisent le préfixe suivant avant l'action : `codestar-notifications and codestar-connections`. Par exemple, pour accorder à une personne l'autorisation d'afficher toutes les règles de notification de son compte, vous incluez l'action `codestar-notifications:ListNotificationRules` dans sa stratégie. Les déclarations de politique doivent inclure un `NotAction` élément `Action` ou. AWS CodeStar Notifications et AWS CodeStar connexions définit son propre ensemble d'actions décrivant les tâches que vous pouvez effectuer avec ce service.

Pour spécifier plusieurs actions de AWS CodeStar notification dans une seule instruction, séparez-les par des virgules comme suit.

```
"Action": [
      "codestar-notifications:action1",
      "codestar-notifications:action2"
```

Pour spécifier plusieurs AWS CodeConnections actions dans une seule instruction, séparez-les par des virgules comme suit.

```
"Action": [
      "codestar-connections:action1",
      "codestar-connections:action2"
```

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

```
"Action": "codestar-notifications:List*"
```

AWS CodeStar Les actions de l'API de notifications incluent :

- `CreateNotificationRule`
- `DeleteNotificationRule`
- `DeleteTarget`
- `DescribeNotificationRule`
- `ListEventTypes`
- `ListNotificationRules`
- `ListTagsForResource`
- `ListTargets`
- `Subscribe`
- `TagResource`
- `Unsubscribe`
- `UntagResource`

- `UpdateNotificationRule`

AWS CodeConnections Les actions de l'API sont les suivantes :

- `CreateConnection`
- `DeleteConnection`
- `GetConnection`
- `ListConnections`
- `ListTagsForResource`
- `TagResource`
- `UntagResource`

Les actions suivantes, basées uniquement sur les autorisations, sont requises AWS CodeConnections pour terminer la poignée de main d'authentification :

- `GetIndividualAccessToken`
- `GetInstallationUrl`
- `ListInstallationTargets`
- `StartOAuthHandshake`
- `UpdateConnectionInstallation`

L'action suivante, basée uniquement sur les autorisations, est requise AWS CodeConnections pour utiliser une connexion :

- `UseConnection`

L'action suivante, basée uniquement sur les autorisations, est requise AWS CodeConnections pour transmettre une connexion à un service :

- `PassConnection`

Pour consulter la liste des actions relatives aux AWS CodeStar notifications et aux AWS CodeStar connexions, consultez les sections Actions définies par AWS CodeStar des notifications et Actions définies par des AWS CodeStar connexions dans le guide de l'utilisateur IAM.

Ressources

AWS CodeStar Les notifications et AWS CodeStar les connexions ne permettent pas de spécifier les ARN des ressources dans une politique.

Clés de condition

AWS CodeStar Les notifications et AWS CodeStar les connexions définissent leurs propres ensembles de clés de condition et prennent également en charge l'utilisation de certaines clés de condition globales. Pour voir toutes les clés de condition AWS globales, voir les clés de contexte de condition AWS globales dans le guide de l'utilisateur IAM.

Toutes les actions de AWS CodeStar notification prennent en charge la clé de `codestar-notifications:NotificationsForResource` condition. Pour plus d'informations, consultez Exemples de politiques basées sur l'identité.

AWS CodeConnections définissez les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus d'informations, consultez AWS CodeConnections référence aux autorisations.

Clés de condition	Description
`codestar-connections:BranchName`	Filtre l'accès en fonction du nom de la branche du référentiel tiers.
`codestar-connections:FullRepositoryId`	Filtre l'accès en fonction du référentiel transmis dans la demande. S'applique uniquement aux demandes `UseConnection` pour l'accès à un référentiel spécifique
`codestar-connections:InstallationId`	Filtre l'accès en fonction de l'ID tiers (tel que l'ID d'installation de l'application Bitbucket) qui est utilisé pour mettre à jour une connexion. Permet de restreindre les installations d'applications tierces qui peuvent être utilisées pour établir une connexion

Clés de condition	Description
`codestar-connections:OwnerId`	Filtre l'accès en fonction du propriétaire ou de l'ID de compte du fournisseur tiers
`codestar-connections:PassedToService`	Filtre l'accès en fonction du service auquel le principal est autorisé à transmettre une connexion
`codestar-connections:ProviderAction`	Filtre l'accès en fonction de l'action du fournisseur dans une demande `UseConnection` telle que `ListRepositories` .
`codestar-connections:ProviderPermissionsRequired`	Filtre l'accès en fonction du type d'autorisations de fournisseur tiers
`codestar-connections:ProviderType`	Filtre l'accès en fonction du type de fournisseur tiers transmis dans la demande
`codestar-connections:ProviderTypeFilter`	Filtre l'accès en fonction du type de fournisseur tiers utilisé pour filtrer les résultats
`codestar-connections:RepositoryName`	Filtre l'accès en fonction du nom du référentiel tiers

Exemples

Pour consulter des exemples de politiques basées sur l'identité relatives aux AWS CodeStar notifications et aux AWS CodeStar connexions, consultez. Exemples de politiques basées sur l'identité

AWS CodeStar Politiques basées sur les ressources relatives aux notifications et aux AWS CodeStar connexions

AWS CodeStar Les notifications et AWS CodeStar les connexions ne prennent pas en charge les politiques basées sur les ressources.

Autorisation basée sur les balises

Vous pouvez associer des balises aux ressources AWS CodeStar Notifications et AWS CodeStar connexions ou transmettre des balises dans une demande. Pour contrôler l'accès basé sur des étiquettes, vous devez fournir les informations d'étiquette dans l'élément de condition d'une politique utilisant les clés de condition `codestar-notifications and codestar-connections:ResourceTag/`*`key-name`*, `aws:RequestTag/`*`key-name`* ou `aws:TagKeys`. Pour plus d'informations sur les stratégies de balisage, consultez la section Ressources de balisage. AWS Pour plus d'informations sur le balisage AWS CodeStar des ressources relatives aux notifications et aux AWS CodeStar connexions, consultezBalisage des ressources de connexions.

Pour visualiser un exemple de stratégie basée sur l'identité permettant de limiter l'accès à une ressource en fonction des balises de cette ressource, veuillez consulter Utilisation de balises pour contrôler l'accès aux ressources AWS CodeStar Connections.

Rôles IAM

Un rôle IAM est une entité de votre AWS compte qui possède des autorisations spécifiques.

Utilisation d'informations d'identification temporaires

Vous pouvez utiliser des informations d'identification temporaires pour vous connecter à la fédération ou endosser un rôle IAM ou un rôle entre comptes. Vous obtenez des informations d'identification de sécurité temporaires en appelant des opérations d' AWS STS API telles que AssumeRoleou GetFederationToken.

AWS CodeStar Notifications and AWS CodeStar Connections prend en charge l'utilisation d'informations d'identification temporaires.

Rôles liés à un service

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

AWS CodeStar Les notifications prennent en charge les rôles liés aux services. Pour plus de détails sur la création ou la gestion AWS CodeStar des rôles liés AWS CodeStar au service Notifications et connexions, consultez. Utilisation de rôles liés à un service pour AWS CodeStar Notifications

AWS CodeStar Connections ne prend pas en charge les rôles liés à un service.

AWS CodeConnections référence aux autorisations

Les tableaux suivants répertorient chaque opération d' AWS CodeConnections API, les actions correspondantes pour lesquelles vous pouvez accorder des autorisations et le format de l'ARN de la ressource à utiliser pour accorder des autorisations. Les AWS CodeConnections API sont regroupées dans des tableaux en fonction de l'étendue des actions autorisées par cette API. Utilisez-le comme référence lorsque vous écrivez des stratégies d'autorisation que vous pouvez attacher à une identité IAM (stratégies basées sur une identité).

Lorsque vous créez une stratégie d'autorisation, vous spécifiez les actions dans le champ `Action` de la stratégie. Vous spécifiez un ARN, avec ou sans caractère générique (*), comme valeur de ressource dans le champ `Resource` de la stratégie.

Pour exprimer des conditions dans les stratégies de connexion, vous pouvez utiliser les clés de condition décrites ici et répertoriées dans Clés de condition. Vous pouvez également utiliser des AWS clés de condition larges. Pour obtenir la liste complète des touches AWS-wide, consultez la section Clés disponibles dans le guide de l'utilisateur IAM.

Pour spécifier une action, utilisez le préfixe `codestar-connections:` suivi du nom de l'opération d'API (par exemple, `codestar-connections:ListConnections` ou `codestar-connections:CreateConnection`).

Utilisation de caractères génériques

Pour spécifier plusieurs actions ou ressources, vous pouvez utiliser un caractère générique (*) dans votre ARN. Par exemple, `codestar-connections:*` spécifie toutes les AWS CodeConnections actions et `codestar-connections:Get*` indique toutes les AWS CodeConnections actions commençant par le mot`Get`. L'exemple suivant accorde l'accès à toutes les ressources dont le nom commence par `MyConnection`.

```
arn:aws:codestar-connections:us-west-2:account-ID:connection/*
```

Vous pouvez uniquement utiliser des caractères génériques avec les ressources *`connection`* répertoriées dans le tableau suivant. Vous ne pouvez pas utiliser de caractères génériques avec les ressources *`region`* ou *`account-id`*. Pour plus d'informations sur les caractères génériques, consultez la section Identifiants IAM dans le guide de l'utilisateur IAM.

Rubriques

- Autorisations pour la gestion des connexions
- Autorisations pour la gestion des hôtes
- Autorisations pour établir des connexions
- Autorisations de configuration des hôtes
- Transmission d'une connexion à un service
- Utilisation d'une connexion
- Types d'accès pris en charge pour ProviderAction
- Autorisations prises en charge pour le balisage des ressources de connexion
- Transmission d'une connexion vers un lien de référentiel
- Clé de condition prise en charge pour les liens de référentiel

Autorisations pour la gestion des connexions

Un rôle ou un utilisateur désigné pour utiliser le AWS CLI SDK pour afficher, créer ou supprimer des connexions doit disposer d'autorisations limitées aux suivantes.

> **Note**
>
> Vous ne pouvez établir ou utiliser une connexion dans la console qu'avec les autorisations suivantes. Vous devez ajouter les autorisations dans Autorisations pour établir des connexions.

```
codestar-connections:CreateConnection
codestar-connections:DeleteConnection
codestar-connections:GetConnection
codestar-connections:ListConnections
```

AWS CodeStar Notifications et AWS CodeStar connexions : autorisations requises pour les actions de gestion des connexions

CreateConnection

Action(s) : `codestar-connections:CreateConnection`

Requis pour utiliser la CLI ou la console pour créer une connexion.

Ressource : `arn:aws:codestar-connections:region:account-id:connection/connection-id`

DeleteConnection

Action(s) : `codestar-connections:DeleteConnection`

Requis pour utiliser la CLI ou la console pour supprimer une connexion.

Ressource : `arn:aws:codestar-connections:region:account-id:connection/connection-id`

GetConnection

Action(s) : `codestar-connections:GetConnection`

Requis pour utiliser la CLI ou la console pour afficher les détails sur une connexion.

Ressource : `arn:aws:codestar-connections:region:account-id:connection/connection-id`

ListConnections

Action(s) : `codestar-connections:ListConnections`

Requis pour utiliser la CLI ou la console pour répertorier toutes les connexions dans le compte.

Ressource : `arn:aws:codestar-connections:region:account-id:connection/connection-id`

Ces opérations prennent en charge les clés de condition suivantes :

Action	Clés de condition
`codestar-connections:CreateConnection`	`codestar-connections:ProviderType`
`codestar-connections:DeleteConnection`	N/A
`codestar-connections:GetConnection`	N/A

Action	Clés de condition
codestar-connections:ListConnections	codestar-connections:ProviderTypeFilter

Autorisations pour la gestion des hôtes

Un rôle ou un utilisateur désigné pour utiliser le AWS CLI SDK pour afficher, créer ou supprimer des hôtes doit disposer d'autorisations limitées aux suivantes.

> **Note**
>
> Vous ne pouvez établir ou utiliser une connexion dans l'hôte qu'avec les autorisations suivantes. Vous devez ajouter les autorisations dans Autorisations de configuration des hôtes.

```
codestar-connections:CreateHost
codestar-connections:DeleteHost
codestar-connections:GetHost
codestar-connections:ListHosts
```

AWS CodeStar Notifications et AWS CodeStar connexions : autorisations requises pour les actions de gestion des hôtes

CreateHost

Action(s) : `codestar-connections:CreateHost`

Requis pour utiliser la CLI ou la console pour créer un hôte.

Ressource :`arn:aws:codestar-connections:`*`region`*`:`*`account-id`*`:host/`*`host-id`*

DeleteHost

Action(s) : `codestar-connections:DeleteHost`

Requis pour utiliser la CLI ou la console pour supprimer un hôte.

Ressource :`arn:aws:codestar-connections:`*`region`*`:`*`account-id`*`:host/`*`host-id`*

GetHost

Action(s) : `codestar-connections:GetHost`

Requis pour utiliser la CLI ou la console pour afficher les détails sur un hôte.

Ressource :`arn:aws:codestar-connections:`*`region`*`:`*`account-id`*`:host/`*`host-id`*

ListHosts

Action(s) : `codestar-connections:ListHosts`

Requis pour utiliser la CLI ou la console pour répertorier toutes les hôtes dans le compte.

Ressource :`arn:aws:codestar-connections:`*`region`*`:`*`account-id`*`:host/`*`host-id`*

Ces opérations prennent en charge les clés de condition suivantes :

Action	Clés de condition
`codestar-connections:CreateHost`	`codestar-connections:ProviderType`
`codestar-connections:DeleteHost`	N/A
`codestar-connections:GetHost`	N/A
`codestar-connections:ListHosts`	`codestar-connections:ProviderTypeFilter`

Autorisations pour établir des connexions

Un rôle ou un utilisateur désigné pour gérer les connexions dans la console doit disposer des autorisations requises pour établir une connexion dans la console et créer une installation, ce qui inclut l'autorisation de négocier avec le fournisseur et de créer des installations pour l'utilisation des connexions. Utilisez les autorisations suivantes en plus des autorisations ci-dessus.

Les opérations IAM suivantes sont utilisées par la console lors de l'exécution d'un processus de négociation basé sur un navigateur. Les `ListInstallationTargets`, `GetInstallationUrl`,

`StartOAuthHandshake`, `UpdateConnectionInstallation` et `GetIndividualAccessToken` sont des autorisations de stratégie IAM. Ce ne sont pas des actions d'API.

```
codestar-connections:GetIndividualAccessToken
codestar-connections:GetInstallationUrl
codestar-connections:ListInstallationTargets
codestar-connections:StartOAuthHandshake
codestar-connections:UpdateConnectionInstallation
```

Sur la base de ces informations, les autorisations suivantes sont nécessaires pour utiliser, créer, mettre à jour ou supprimer une connexion dans la console.

```
codestar-connections:CreateConnection
codestar-connections:DeleteConnection
codestar-connections:GetConnection
codestar-connections:ListConnections
codestar-connections:UseConnection
codestar-connections:ListInstallationTargets
codestar-connections:GetInstallationUrl
codestar-connections:StartOAuthHandshake
codestar-connections:UpdateConnectionInstallation
codestar-connections:GetIndividualAccessToken
```

AWS CodeConnections autorisations requises pour les actions permettant d'établir des connexions

GetIndividualAccessToken

Action(s) : `codestar-connections:GetIndividualAccessToken`

Requise pour utiliser la console pour établir une connexion. Il s'agit d'une autorisation de stratégie IAM uniquement, pas d'une action d'API.

Ressource :`arn:aws:codestar-connections:`*`region`*`:`*`account-id`*`:connection/`*`connection-id`*

GetInstallationUrl

Action(s) : `codestar-connections:GetInstallationUrl`

Requise pour utiliser la console pour établir une connexion. Il s'agit d'une autorisation de stratégie IAM uniquement, pas d'une action d'API.

Ressource : `arn:aws:codestar-connections:region:account-id:connection/connection-id`

ListInstallationTargets

Action(s) : `codestar-connections:ListInstallationTargets`

Requise pour utiliser la console pour établir une connexion. Il s'agit d'une autorisation de stratégie IAM uniquement, pas d'une action d'API.

Ressource : `arn:aws:codestar-connections:region:account-id:connection/connection-id`

Commencer à AuthHandshake

Action(s) : `codestar-connections:StartOAuthHandshake`

Requise pour utiliser la console pour établir une connexion. Il s'agit d'une autorisation de stratégie IAM uniquement, pas d'une action d'API.

Ressource : `arn:aws:codestar-connections:region:account-id:connection/connection-id`

UpdateConnectionInstallation

Action(s) : `codestar-connections:UpdateConnectionInstallation`

Requise pour utiliser la console pour établir une connexion. Il s'agit d'une autorisation de stratégie IAM uniquement, pas d'une action d'API.

Ressource : `arn:aws:codestar-connections:region:account-id:connection/connection-id`

Ces opérations prennent en charge les clés de condition suivantes.

Action	Clés de condition
`codestar-connections:GetIndividualAccessToken`	`codestar-connections:ProviderType`
`codestar-connections:GetInstallationUrl`	`codestar-connections:ProviderType`

Action	Clés de condition
codestar-connections:ListInstallationTargets	N/A
codestar-connections:StartOAuthHandshake	codestar-connections:ProviderType
codestar-connections:UpdateConnectionInstallation	codestar-connections:InstallationId

Autorisations de configuration des hôtes

Un rôle ou un utilisateur désigné pour gérer les connexions dans la console doit disposer des autorisations requises pour configurer un hôte dans la console, ce qui inclut l'autorisation de négocier avec le fournisseur et d'installer pour l'application de l'hôte. Utilisez les autorisations suivantes en plus des autorisations pour hôtes ci-dessus.

Les opérations IAM suivantes sont utilisées par la console lors de l'enregistrement d'hôte basé sur un navigateur. `RegisterAppCode` et `StartAppRegistrationHandshake` sont des autorisations de stratégie IAM. Ce ne sont pas des actions d'API.

```
codestar-connections:RegisterAppCode
codestar-connections:StartAppRegistrationHandshake
```

Sur la base de ces informations, les autorisations suivantes sont nécessaires pour utiliser, créer, mettre à jour ou supprimer une connexion dans la console qui nécessite un hôte (comme les types de fournisseurs installés).

```
codestar-connections:CreateConnection
codestar-connections:DeleteConnection
codestar-connections:GetConnection
codestar-connections:ListConnections
codestar-connections:UseConnection
codestar-connections:ListInstallationTargets
codestar-connections:GetInstallationUrl
codestar-connections:StartOAuthHandshake
codestar-connections:UpdateConnectionInstallation
```

```
codestar-connections:GetIndividualAccessToken
codestar-connections:RegisterAppCode
codestar-connections:StartAppRegistrationHandshake
```

AWS CodeConnections autorisations requises pour les actions permettant de terminer la configuration de l'hôte

RegisterAppCode

Action(s) : `codestar-connections:RegisterAppCode`

Requis pour utiliser la console pour finaliser la configuration de l'hôte. Il s'agit d'une autorisation de stratégie IAM uniquement, pas d'une action d'API.

Ressource :`arn:aws:codestar-connections:`*`region`*`:`*`account-id`*`:host/`*`host-id`*

StartAppRegistrationHandshake

Action(s) : `codestar-connections:StartAppRegistrationHandshake`

Requis pour utiliser la console pour finaliser la configuration de l'hôte. Il s'agit d'une autorisation de stratégie IAM uniquement, pas d'une action d'API.

Ressource :`arn:aws:codestar-connections:`*`region`*`:`*`account-id`*`:host/`*`host-id`*

Ces opérations prennent en charge les clés de condition suivantes.

Transmission d'une connexion à un service

Lorsqu'une connexion est transmise à un service (par exemple, lorsqu'un ARN de connexion est fourni dans une définition de pipeline pour créer ou mettre à jour un pipeline), l'utilisateur doit disposer de l'autorisation `codestar-connections:PassConnection`.

AWS CodeConnections autorisations requises pour passer une connexion

PassConnection

Action(s) : `codestar-connections:PassConnection`

Requis pour transférer une connexion à un service.

Ressource :`arn:aws:codestar-connections:`*`region`*`:`*`account-id`*`:connection/`*`connection-id`*

Cette opération prend également en charge la clé de condition suivante :

- `codestar-connections:PassedToService`

Valeurs prises en charge pour les clés de condition

Clé	Fournisseurs d'actions valides
`codestar-connections:PassedToService`	• `codeguru-reviewer` • `codepipeline.amazonaws.com` • `proton.amazonaws.com`

Utilisation d'une connexion

Lorsqu'un service tel que celui-ci CodePipeline utilise une connexion, le rôle de service doit disposer de l'`codestar-connections:UseConnection`autorisation pour une connexion donnée.

Pour gérer les connexions de la console, la stratégie utilisateur doit avoir l'autorisation `codestar-connections:UseConnection`.

AWS CodeConnections action requise pour utiliser une connexion

UseConnection

Action(s) : `codestar-connections:UseConnection`

Requis pour utiliser une connexion.

Ressource :`arn:aws:codestar-connections:`*`region`*`:`*`account-id`*`:connection/`*`connection-id`*

Cette opération prend également en charge les clés de condition suivantes :

- `codestar-connections:BranchName`
- `codestar-connections:FullRepositoryId`
- `codestar-connections:OwnerId`
- `codestar-connections:ProviderAction`
- `codestar-connections:ProviderPermissionsRequired`

- `codestar-connections:RepositoryName`

Valeurs prises en charge pour les clés de condition

Clé	Fournisseurs d'actions valides
`codestar-connections:FullRepositoryId`	Nom de l'utilisateur et nom d'un référentiel, par exemple `my-owner/my-repository` . Prise en charge uniquement lorsque la connexion est utilisée pour accéder à un référentiel spécifique.
`codestar-connections:ProviderPermissionsRequired`	read_only ou read_write
`codestar-connections:ProviderAction`	`GetBranch` , `ListRepositories` , `ListOwners` , `ListBranches` , `StartUploadArchiveToS3` , `GitPush`, `GitPull`, `GetUploadArchiveToS3Status` , `CreatePullRequestDiffComment` , `GetPullRequest` , `ListBranchCommits` , `ListCommitFiles` , `ListPullRequestComments` , `ListPullRequestCommits` . Pour plus d'informations, consultez la section suivante.

Les clés de condition requises pour certaines fonctionnalités peuvent changer au fil du temps. Nous vous recommandons d'utiliser `codestar-connections:UseConnection` pour contrôler l'accès à une connexion, sauf si vos exigences de contrôle d'accès requièrent des autorisations différentes.

Types d'accès pris en charge pour **`ProviderAction`**

Lorsqu'une connexion est utilisée par un AWS service, des appels d'API sont effectués vers votre fournisseur de code source. Par exemple, un service peut répertorier les référentiels pour une connexion Bitbucket en appelant l'API `https://api.bitbucket.org/2.0/repositories/`*`username`*.

La clé de condition `ProviderAction` vous permet de restreindre les API d'un fournisseur qui peuvent être appelées. Comme le chemin de l'API peut être généré dynamiquement et que le chemin varie d'un fournisseur à l'autre, la valeur `ProviderAction` est mappée à un nom d'action abstrait plutôt qu'à l'URL de l'API. Cela vous permet d'écrire des stratégies qui ont le même effet quel que soit le type de fournisseur de la connexion.

Voici les types d'accès qui sont accordés pour chacune des valeurs `ProviderAction` prises en charge. Voici des autorisations de stratégie IAM. Ce ne sont pas des actions d'API.

AWS CodeConnections types d'accès pris en charge pour **`ProviderAction`**

GetBranch

Action(s) : `codestar-connections:GetBranch`

Requis pour accéder aux informations d'une branche, telles que la dernière validation de cette branche.

Ressource :`arn:aws:codestar-connections:`*`region`*`:`*`account-id`*`:connection/`*`connection-id`*

ListRepositories

Action(s) : `codestar-connections:ListRepositories`

Requis pour accéder à une liste de référentiels publics et privés qui appartiennent à un propriétaire, ainsi qu'aux détails sur ces référentiels.

Ressource :`arn:aws:codestar-connections:`*`region`*`:`*`account-id`*`:connection/`*`connection-id`*

ListOwners

Action(s) : `codestar-connections:ListOwners`

Requis pour accéder à la liste des propriétaires auxquels la connexion a accès.

Ressource :`arn:aws:codestar-connections:`*`region`*`:`*`account-id`*`:connection/`*`connection-id`*

ListBranches

Action(s) : `codestar-connections:ListBranches`

Requis pour accéder à la liste des branches qui existent sur un référentiel donné.

Ressource :`arn:aws:codestar-connections:`*`region`*`:`*`account-id`*`:connection/`*`connection-id`*

StartUploadArchiveToS3

Action(s) : `codestar-connections:StartUploadArchiveToS3`

Requis pour lire le code source et le télécharger sur Amazon S3.

Ressource :`arn:aws:codestar-connections:`*`region`*`:`*`account-id`*`:connection/`*`connection-id`*

GitPush

Action(s) : `codestar-connections:GitPush`

Requis pour écrire dans un référentiel à l'aide de Git.

Ressource :`arn:aws:codestar-connections:`*`region`*`:`*`account-id`*`:connection/`*`connection-id`*

GitPull

Action(s) : `codestar-connections:GitPull`

Requis pour lire les données d'un référentiel à l'aide de Git.

Ressource :`arn:aws:codestar-connections:`*`region`*`:`*`account-id`*`:connection/`*`connection-id`*

GetUploadArchiveToÉtat S3

Action(s) : `codestar-connections:GetUploadArchiveToS3Status`

Requis pour accéder à l'état d'un chargement, y compris aux messages d'erreur par `StartUploadArchiveToS3`.

Ressource :`arn:aws:codestar-connections:`*`region`*`:`*`account-id`*`:connection/`*`connection-id`*

CreatePullRequestDiffComment

Action(s) : `codestar-connections:CreatePullRequestDiffComment`

Requis pour accéder aux commentaires sur une demande d'extraction.

Ressource :`arn:aws:codestar-connections:`*`region`*`:`*`account-id`*`:connection/`*`connection-id`*

GetPullRequest

Action(s) : `codestar-connections:GetPullRequest`

Requis pour afficher les demandes d'extraction d'un référentiel.

Ressource :`arn:aws:codestar-connections:`*`region`*`:`*`account-id`*`:connection/`*`connection-id`*

ListBranchCommits

Action(s) : `codestar-connections:ListBranchCommits`

Requis pour afficher une liste de validations pour une branche du référentiel.

Ressource :`arn:aws:codestar-connections:`*`region`*`:`*`account-id`*`:connection/`*`connection-id`*

ListCommitFiles

Action(s) : `codestar-connections:ListCommitFiles`

Requis pour afficher une liste de fichiers pour une validation.

Ressource :`arn:aws:codestar-connections:`*`region`*`:`*`account-id`*`:connection/`*`connection-id`*

ListPullRequestComments

Action(s) : `codestar-connections:ListPullRequestComments`

Requis pour afficher une liste de commentaires pour une demande d'extraction.

Ressource :`arn:aws:codestar-connections:`*`region`*`:`*`account-id`*`:connection/`*`connection-id`*

ListPullRequestCommits

Action(s) : `codestar-connections:ListPullRequestCommits`

Requis pour afficher une liste de validations pour une requête d'extraction.

Ressource : `arn:aws:codestar-connections:region:account-id:connection/connection-id`

Autorisations prises en charge pour le balisage des ressources de connexion

Les opérations IAM suivantes sont utilisées lors du balisage des ressources de connexion.

```
codestar-connections:ListTagsForResource
codestar-connections:TagResource
codestar-connections:UntagResource
```

AWS CodeConnections actions requises pour le balisage des ressources de connexion

ListTagsForResource

Action(s) : `codestar-connections:ListTagsForResource`

Requis pour afficher une liste des balises associées à la ressource de connexion.

Ressource : `arn:aws:codestar-connections:region:account-id:connection/connection-id`, `arn:aws:codestar-connections:region:account-id:host/host-id`

TagResource

Action(s) : `codestar-connections:TagResource`

Requis pour baliser une ressource de connexion.

Ressource : `arn:aws:codestar-connections:region:account-id:connection/connection-id`,

UntagResource

Action(s) : `codestar-connections:UntagResource`

Autorisation requise pour supprimer des balises d'une ressource de connexion.

Ressource : `arn:aws:codestar-connections:region:account-id:connection/connection-id`, `arn:aws:codestar-connections:region:account-id:host/host-id`

Transmission d'une connexion vers un lien de référentiel

Lorsqu'un lien de référentiel est fourni dans une configuration de synchronisation, l'utilisateur doit avoir l'autorisation `codestar-connections:PassRepository` pour l'ARN/la ressource du lien de référentiel.

AWS CodeConnections autorisations requises pour passer une connexion

PassRepository

Action(s) : `codestar-connections:PassRepository`

Nécessaire pour transmettre un lien de référentiel à une configuration de synchronisation.

Ressource :`arn:aws:codestar-connections:`*`region`*`:`*`account-id`*`:repository-link/`*`repository-link-id`*

Cette opération prend également en charge la clé de condition suivante :

- `codestar-connections:PassedToService`

Valeurs prises en charge pour les clés de condition

Clé	Fournisseurs d'actions valides
`codestar-connections:PassedToService`	• `cloudformation.sync.codeconnections.amazonaws.com`

Clé de condition prise en charge pour les liens de référentiel

Les opérations relatives aux liens de référentiel et aux ressources de configuration de synchronisation sont prises en charge par la clé de condition suivante :

- `codestar-connections:Branch`

  Filtre l'accès en fonction du nom de la branche transmis dans la demande.

Actions prises en charge pour la clé de condition

Clé	Valeurs valides
`codestar-connections:Branch`	Les actions suivantes sont prises en charge pour cette clé de condition : • CreateSyncConfiguration • UpdateSyncConfiguration • GetRepositorySyncStatus

Exemples de politiques basées sur l'identité

Par défaut, les utilisateurs et les rôles IAM dotés de l'une des politiques gérées pour AWS CodeCommit AWS CodeBuild AWS CodeDeploy, ou AWS CodePipeline appliquées disposent d'autorisations relatives aux connexions, aux notifications et aux règles de notification conformes à l'intention de ces politiques. Par exemple, les utilisateurs ou rôles IAM auxquels l'une des politiques d'accès complet (AWSCodeCommitFullAccess,, AWSCodeBuildAdminAccessAWSCodeDeployFullAccess, ou AWSCodePipeline_FullAccess) leur est appliquée ont également un accès complet aux notifications et aux règles de notification créées pour les ressources de ces services.

Les autres utilisateurs et rôles IAM ne sont pas autorisés à créer ou à modifier les ressources de AWS CodeStar notifications et de AWS CodeStar connexions. Ils ne peuvent pas non plus effectuer de tâches à l'aide de l' AWS API AWS Management Console AWS CLI, ou. Un administrateur IAM doit créer des stratégies IAM autorisant les utilisateurs et les rôles à exécuter des opérations d'API sur les ressources spécifiées dont ils ont besoin. Il doit ensuite attacher ces politiques aux utilisateurs ou aux groupes IAM ayant besoin de ces autorisations.

Autorisations et exemples pour les AWS CodeStar notifications

Les déclarations de politique et les exemples suivants peuvent vous aider à gérer les AWS CodeStar notifications.

Autorisations liées aux notifications dans les stratégies gérées d'accès complet

Les politiques AWSCodeCommitFullAccessAWSCodeBuildAdminAccess, AWSCodeDeployFullAccess, et AWSCodePipeline_FullAccessgérées incluent les instructions suivantes pour permettre un accès complet aux notifications dans la console Developer Tools. Les

utilisateurs auxquels l'une de ces stratégies gérées est appliquée peuvent également créer et gérer des rubriques Amazon SNS pour les notifications, abonner et désabonner les utilisateurs à des rubriques et répertorier les rubriques à choisir comme cibles pour les règles de notification.

> **Note**
>
> Dans la stratégie gérée, la clé de condition `codestar-notifications:NotificationsForResource` a une valeur spécifique au type de ressource du service. Par exemple, dans la politique d'accès complet pour CodeCommit, la valeur est`arn:aws:codecommit:*`.

```
    {
        "Sid": "CodeStarNotificationsReadWriteAccess",
        "Effect": "Allow",
        "Action": [
            "codestar-notifications:CreateNotificationRule",
            "codestar-notifications:DescribeNotificationRule",
            "codestar-notifications:UpdateNotificationRule",
            "codestar-notifications:DeleteNotificationRule",
            "codestar-notifications:Subscribe",
            "codestar-notifications:Unsubscribe"
        ],
        "Resource": "*",
        "Condition" : {
            "StringLike" : {"codestar-notifications:NotificationsForResource" :
"arn:aws:<vendor-code>:*"}
        }
    },
    {
        "Sid": "CodeStarNotificationsListAccess",
        "Effect": "Allow",
        "Action": [
            "codestar-notifications:ListNotificationRules",
            "codestar-notifications:ListTargets",
            "codestar-notifications:ListTagsforResource",
            "codestar-notifications:ListEventTypes"
        ],
        "Resource": "*"
    },
    {
        "Sid": "CodeStarNotificationsSNSTopicCreateAccess",
```

```
        "Effect": "Allow",
        "Action": [
            "sns:CreateTopic",
            "sns:SetTopicAttributes"
        ],
        "Resource": "arn:aws:sns:*:*:codestar-notifications*"
    },
    {
        "Sid": "SNSTopicListAccess",
        "Effect": "Allow",
        "Action": [
            "sns:ListTopics"
        ],
        "Resource": "*"
    },
    {
        "Sid": "CodeStarNotificationsChatbotAccess",
        "Effect": "Allow",
        "Action": [
            "chatbot:DescribeSlackChannelConfigurations",
            "chatbot:ListMicrosoftTeamsChannelConfigurations"
          ],
       "Resource": "*"
    }
```

Autorisations liées aux notifications dans les stratégies gérées en lecture seule

Les politiques AWSCodeCommitReadOnlyAccessAWSCodeBuildReadOnlyAccess, AWSCodeDeployReadOnlyAccess, et AWSCodePipeline_ReadOnlyAccessgérées incluent les instructions suivantes pour autoriser l'accès en lecture seule aux notifications. Par exemple, elles peuvent afficher des notifications pour les ressources dans la console Outils pour développeurs, mais ne peuvent pas les créer, les gérer ou s'y abonner.

> **Note**
>
> Dans la stratégie gérée, la clé de condition `codestar-notifications:NotificationsForResource` a une valeur spécifique au type de ressource du service. Par exemple, dans la politique d'accès complet pour CodeCommit, la valeur est`arn:aws:codecommit:*`.

```
  {
       "Sid": "CodeStarNotificationsPowerUserAccess",
       "Effect": "Allow",
       "Action": [
           "codestar-notifications:DescribeNotificationRule"
       ],
       "Resource": "*",
       "Condition" : {
           "StringLike" : {"codestar-notifications:NotificationsForResource" :
"arn:aws:<vendor-code>:*"}
       }
   },
   {
       "Sid": "CodeStarNotificationsListAccess",
       "Effect": "Allow",
       "Action": [
           "codestar-notifications:ListNotificationRules",
           "codestar-notifications:ListEventTypes",
           "codestar-notifications:ListTargets"
       ],
       "Resource": "*"
   }
```

Autorisations liées aux notifications dans d'autres stratégies gérées

Les politiques AWSCodeCommitPowerUserAWSCodeBuildDeveloperAccess, et AWSCodeBuildDeveloperAccessgérées incluent les instructions suivantes pour permettre aux développeurs appliquant l'une de ces politiques gérées de créer, de modifier et de s'abonner à des notifications. Ils ne peuvent pas supprimer les règles de notification ni gérer les balises pour les ressources.

> **Note**
>
> Dans la stratégie gérée, la clé de condition `codestar-notifications:NotificationsForResource` a une valeur spécifique au type de ressource du service. Par exemple, dans la politique d'accès complet pour CodeCommit, la valeur est`arn:aws:codecommit:*`.

```
   {
       "Sid": "CodeStarNotificationsReadWriteAccess",
```

```
        "Effect": "Allow",
        "Action": [
            "codestar-notifications:CreateNotificationRule",
            "codestar-notifications:DescribeNotificationRule",
            "codestar-notifications:UpdateNotificationRule",
            "codestar-notifications:Subscribe",
            "codestar-notifications:Unsubscribe"
        ],
        "Resource": "*",
        "Condition" : {
            "StringLike" : {"codestar-notifications:NotificationsForResource" :
"arn:aws:<vendor-code>:*"}
        }
    },
    {
        "Sid": "CodeStarNotificationsListAccess",
        "Effect": "Allow",
        "Action": [
            "codestar-notifications:ListNotificationRules",
            "codestar-notifications:ListTargets",
            "codestar-notifications:ListTagsforResource",
            "codestar-notifications:ListEventTypes"
        ],
        "Resource": "*"
    },
    {
        "Sid": "SNSTopicListAccess",
        "Effect": "Allow",
        "Action": [
            "sns:ListTopics"
        ],
        "Resource": "*"
    },
    {
        "Sid": "CodeStarNotificationsChatbotAccess",
        "Effect": "Allow",
        "Action": [
            "chatbot:DescribeSlackChannelConfigurations",
            "chatbot:ListMicrosoftTeamsChannelConfigurations"
          ],
       "Resource": "*"
    }
```

Exemple : politique de gestion des notifications au niveau de l'administrateur AWS CodeStar

Dans cet exemple, vous souhaitez accorder à un utilisateur IAM de votre AWS compte un accès complet aux AWS CodeStar notifications afin qu'il puisse consulter les détails des règles de notification et répertorier les règles de notification, les cibles et les types d'événements. Vous souhaitez également autoriser l'utilisateur à ajouter, mettre à jour et supprimer des règles de notification. Il s'agit d'une politique d'accès complet, équivalente aux autorisations de notification incluses dans les politiques AWSCodeBuildAdminAccessAWSCodeCommitFullAccessAWSCodeDeployFullAccess,, et AWSCodePipeline_FullAccessgérées. À l'instar de ces politiques gérées, vous ne devez associer ce type de déclaration de politique qu'aux utilisateurs, groupes ou rôles IAM qui nécessitent un accès administratif complet aux notifications et aux règles de notification de votre AWS compte.

> **Note**
>
> Cette stratégie contient les autorisations `CreateNotificationRule`. Tout utilisateur dont cette politique est appliquée à son utilisateur ou à son rôle IAM pourra créer des règles de notification pour tous les types de ressources pris en charge par les AWS CodeStar notifications dans le AWS compte, même s'il n'a pas accès à ces ressources lui-même. Par exemple, un utilisateur appliquant cette politique peut créer une règle de notification pour un CodeCommit référentiel sans être autorisé à y CodeCommit accéder.

```
{
    "Version": "2012-10-17",
    "Statement": [
      {
        "Sid": "AWSCodeStarNotificationsFullAccess",
        "Effect": "Allow",
        "Action": [
            "codestar-notifications:CreateNotificationRule",
            "codestar-notifications:DeleteNotificationRule",
            "codestar-notifications:DescribeNotificationRule",
            "codestar-notifications:ListNotificationRules",
            "codestar-notifications:UpdateNotificationRule",
            "codestar-notifications:Subscribe",
            "codestar-notifications:Unsubscribe",
            "codestar-notifications:DeleteTarget",
            "codestar-notifications:ListTargets",
            "codestar-notifications:ListTagsforResource",
```

```
            "codestar-notifications:TagResource",
            "codestar-notifications:UntagResource"
        ],
        "Resource": "*"
      }
   ]
}
```

Exemple : politique d'utilisation des notifications au niveau des contributeurs AWS CodeStar

Dans cet exemple, vous souhaitez autoriser l'accès à l' day-to-day utilisation des AWS CodeStar notifications, telles que la création de notifications et l'abonnement à celles-ci, mais pas à des actions plus destructrices, telles que la suppression de règles ou de cibles de notification. C'est l'équivalent de l'accès fourni dans les politiques AWSCodeBuildDeveloperAccessAWSCodeDeployDeveloperAccess, et AWSCodeCommitPowerUsergérées.

> **Note**
>
> Cette stratégie contient les autorisations `CreateNotificationRule`. Tout utilisateur dont cette politique est appliquée à son utilisateur ou à son rôle IAM pourra créer des règles de notification pour tous les types de ressources pris en charge par les AWS CodeStar notifications dans le AWS compte, même s'il n'a pas accès à ces ressources lui-même. Par exemple, un utilisateur appliquant cette politique peut créer une règle de notification pour un CodeCommit référentiel sans être autorisé à y CodeCommit accéder.

```
{
    "Version": "2012-10-17",
    "Sid": "AWSCodeStarNotificationsPowerUserAccess",
        "Effect": "Allow",
        "Action": [
            "codestar-notifications:CreateNotificationRule",
            "codestar-notifications:DescribeNotificationRule",
            "codestar-notifications:ListNotificationRules",
            "codestar-notifications:UpdateNotificationRule",
            "codestar-notifications:Subscribe",
            "codestar-notifications:Unsubscribe",
            "codestar-notifications:ListTargets",
            "codestar-notifications:ListTagsforResource"
```

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

Exemple : read-only-level politique d'utilisation AWS CodeStar des notifications

Dans cet exemple, vous souhaitez accorder à un utilisateur IAM de votre compte l'accès en lecture seule aux règles de notification, aux cibles et aux types d'événements de votre compte AWS . Cet exemple montre comment créer une stratégie qui permet d'afficher ces éléments. Cela équivaut aux autorisations incluses dans le cadre des AWSCodeBuildReadOnlyAccesspolitiques AWSCodePipeline_ReadOnlyAccessgérées et des politiques. AWSCodeCommitReadOnly

```
{
    "Version": "2012-10-17",
    "Id": "CodeNotification__ReadOnly",
    "Statement": [
        {
            "Sid": "Reads_API_Access",
            "Effect": "Allow",
            "Action": [
                "CodeNotification:DescribeNotificationRule",
                "CodeNotification:ListNotificationRules",
                "CodeNotification:ListTargets",
                "CodeNotification:ListEventTypes"
            ],
            "Resource": "*"
        }
    ]
}
```

Autorisations et exemples pour AWS CodeConnections

Les déclarations et exemples de politique suivants peuvent vous aider à gérer AWS CodeConnections.

Pour plus d'informations sur la création d'une stratégie basée sur l'identité IAM à l'aide de ces exemples de documents de stratégie JSON, consultez Création de stratégies dans l'onglet JSON dans le guide de l'utilisateur IAM.

Exemple : politique de création à l' AWS CodeConnections aide de la CLI et d'affichage à l'aide de la console

Un rôle ou un utilisateur désigné pour utiliser le AWS CLI SDK pour afficher, créer, étiqueter ou supprimer des connexions doit disposer d'autorisations limitées aux suivantes.

> **Note**
>
> Vous ne pouvez établir une connexion dans la console qu'avec les autorisations suivantes. Vous devez ajouter les autorisations de la section suivante.

Pour utiliser la console dans e but d'afficher une liste des connexions disponibles, d'afficher les balises et d'utiliser une connexion, utilisez la stratégie suivante.

```
{
    "Version": "2012-10-17",
    "Statement": [
      {
        "Sid": "ConnectionsFullAccess",
        "Effect": "Allow",
        "Action": [
            "codestar-connections:CreateConnection",
            "codestar-connections:DeleteConnection",
            "codestar-connections:UseConnection",
            "codestar-connections:GetConnection",
            "codestar-connections:ListConnections",
            "codestar-connections:TagResource",
            "codestar-connections:ListTagsForResource",
            "codestar-connections:UntagResource"
        ],
        "Resource": "*"
      }
   ]
}
```

Exemple : politique de création à l' AWS CodeConnections aide de la console

Un rôle ou un utilisateur désigné pour gérer les connexions dans la console doit disposer des autorisations requises pour établir une connexion dans la console et créer une installation, ce qui inclut l'autorisation de négocier avec le fournisseur et de créer des installations pour l'utilisation des

connexions.`UseConnection` doit également être ajouté pour utiliser la connexion dans la console. Utilisez la stratégie suivante pour afficher, utiliser, créer, étiqueter ou supprimer une connexion dans la console.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "codestar-connections:CreateConnection",
                "codestar-connections:DeleteConnection",
                "codestar-connections:GetConnection",
                "codestar-connections:ListConnections",
                "codestar-connections:GetInstallationUrl",
                "codestar-connections:GetIndividualAccessToken",
                "codestar-connections:ListInstallationTargets",
                "codestar-connections:StartOAuthHandshake",
                "codestar-connections:UpdateConnectionInstallation",
                "codestar-connections:UseConnection",
                "codestar-connections:TagResource",
                "codestar-connections:ListTagsForResource",
                "codestar-connections:UntagResource"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

Exemple : politique de gestion au niveau de l'administrateur AWS CodeConnections

Dans cet exemple, vous souhaitez accorder un accès complet à un utilisateur IAM de votre AWS compte CodeConnections afin qu'il puisse ajouter, mettre à jour et supprimer des connexions. Il s'agit d'une politique d'accès complet, équivalente à la politique AWSCodePipeline_FullAccessgérée. À l'instar de cette politique gérée, vous ne devez associer ce type de déclaration de politique qu'aux utilisateurs, groupes ou rôles IAM qui nécessitent un accès administratif complet aux connexions de votre AWS compte.

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

```
    "Statement": [
      {
        "Sid": "ConnectionsFullAccess",
        "Effect": "Allow",
        "Action": [
            "codestar-connections:CreateConnection",
            "codestar-connections:DeleteConnection",
            "codestar-connections:UseConnection",
            "codestar-connections:GetConnection",
            "codestar-connections:ListConnections",
            "codestar-connections:ListInstallationTargets",
            "codestar-connections:GetInstallationUrl",
            "codestar-connections:StartOAuthHandshake",
            "codestar-connections:UpdateConnectionInstallation",
            "codestar-connections:GetIndividualAccessToken",
            "codestar-connections:TagResource",
            "codestar-connections:ListTagsForResource",
            "codestar-connections:UntagResource"
        ],
        "Resource": "*"
      }
   ]
}
```

Exemple : politique d'utilisation au niveau du contributeur AWS CodeConnections

Dans cet exemple, vous souhaitez autoriser l'accès à l' day-to-day utilisation de CodeConnections, telles que la création et l'affichage des détails des connexions, mais pas à des actions plus destructrices, telles que la suppression de connexions.

```
{
    "Version": "2012-10-17",
    "Sid": "AWSCodeStarConnectionsPowerUserAccess",
        "Effect": "Allow",
        "Action": [
            "codestar-connections:CreateConnection",
            "codestar-connections:UseConnection",
            "codestar-connections:GetConnection",
            "codestar-connections:ListConnections",
            "codestar-connections:ListInstallationTargets",
            "codestar-connections:GetInstallationUrl",
            "codestar-connections:GetIndividualAccessToken",
            "codestar-connections:StartOAuthHandshake",
```

```
            "codestar-connections:UpdateConnectionInstallation",
            "codestar-connections:ListTagsForResource"
        ],
        "Resource": "*"
        }
    ]
}
```

Exemple : read-only-level politique d'utilisation AWS CodeConnections

Dans cet exemple, vous souhaitez accorder à un utilisateur IAM de votre compte un accès en lecture seule aux connexions de votre compte. AWS Cet exemple montre comment créer une stratégie qui permet d'afficher ces éléments.

```
{
    "Version": "2012-10-17",
    "Id": "Connections__ReadOnly",
    "Statement": [
        {
            "Sid": "Reads_API_Access",
            "Effect": "Allow",
            "Action": [
            "codestar-connections:GetConnection",
            "codestar-connections:ListConnections",
            "codestar-connections:ListInstallationTargets",
            "codestar-connections:GetInstallationUrl",
            "codestar-connections:ListTagsForResource"
            ],
            "Resource": "*"
        }
    ]
}
```

Exemple : politique limitée à utiliser AWS CodeConnections avec un référentiel spécifié

Dans l'exemple suivant, le client souhaite que le rôle de CodeBuild service accède au référentiel Bitbucket spécifié. La politique relative au rôle CodeBuild de service :

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Allow",
```

```
        "Action": [
            "codestar-connections:UseConnection"
        ],
        "Resource": "arn:aws:codestar-connections:us-
west-2:connection:3dee99b9-172f-4ebe-a257-722365a39557",
        "Condition": {"ForAllValues:StringEquals": {"codestar-
connections:FullRepositoryId": "myrepoowner/myreponame"}}
    }
}
```

Exemple : politique pour utiliser une connexion avec CodePipeline

Dans l'exemple suivant, un administrateur souhaite que les utilisateurs utilisent une connexion avec CodePipeline. La stratégie attachée à l'utilisateur :

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Action": [
            "codestar-connections:PassConnection"
        ],
        "Resource": "arn:aws:codestar-connections:us-west-2:connection/
aEXAMPLE-8aad-4d5d-8878-dfcab0bc441f",
        "Condition": {"ForAllValues:StringEquals": {"codestar-
connections:PassedToService": "codepipeline.amazonaws.com"}}
    }
}
```

Exemple : utiliser un rôle CodeBuild de service pour les opérations de lecture de Bitbucket avec AWS CodeConnections

Dans l'exemple suivant, le client souhaite que le rôle de CodeBuild service effectue des opérations de lecture sur Bitbucket quel que soit le référentiel. La politique relative au rôle CodeBuild de service :

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Action": [
            "codestar-connections:UseConnection"
        ],
```

```
        "Resource": "arn:aws:codestar-connections:us-west-2:connection/
aEXAMPLE-8aad-4d5d-8878-dfcab0bc441f",
        "Condition": {"ForAllValues:StringEquals": {"codestar-
connections:ProviderPermissionsRequired": "read_only"}}
    }
}
```

Exemple : empêcher le rôle CodeBuild de service d'effectuer des opérations avec AWS CodeConnections

Dans l'exemple suivant, le client souhaite empêcher le rôle de CodeBuild service d'effectuer une opération telle que`CreateRepository`. La politique relative au rôle CodeBuild de service :

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Action": [
            "codestar-connections:UseConnection"
        ],
        "Resource": "arn:aws:codestar-connections:us-west-2:connection/
aEXAMPLE-8aad-4d5d-8878-dfcab0bc441f",
        "Condition": {"ForAllValues:StringNotEquals": {"codestar-
connections:ProviderPermissionsRequired": "CreateRepository"}}
    }
}
```

Utilisation de balises pour contrôler l'accès aux ressources AWS CodeStar Connections

Les balises peuvent être attachées à la ressource ou transmises dans la demande aux services qui prennent en charge le balisage. Dans CodeConnections, les ressources peuvent avoir des balises, et certaines actions peuvent inclure des balises. Lorsque vous créez une stratégie IAM, vous pouvez utiliser des clés de condition de balise pour contrôler les éléments suivants :

- quels utilisateurs peuvent effectuer des actions sur une ressource de pipeline, en fonction des balises que la ressource possède déjà ;
- quelles balises peuvent être transmises dans une demande d'action ;
- si des clés de balise spécifiques peuvent être utilisées dans une demande.

Les exemples suivants montrent comment spécifier des conditions de balises dans les stratégies pour les utilisateurs CodeConnections .

Example 1 : Autoriser des actions en fonction des balises dans la demande

La politique suivante accorde aux utilisateurs l'autorisation de créer des connexions dans CodeConnections.

Pour ce faire, elle autorise les actions `CreateConnection` et `TagResource` si la demande spécifie une balise nommée `Project` avec la valeur `ProjectA`. (La clé de condition `aws:RequestTag` est utilisée pour contrôler les balises qui peuvent être transmises dans une demande IAM.) La condition `aws:TagKeys` garantit que la clé de balise est sensible à la casse.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "codestar-connections:CreateConnection",
        "codestar-connections:TagResource"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:RequestTag/Project": "ProjectA"
        },
        "ForAllValues:StringEquals": {
          "aws:TagKeys": ["Project"]
        }
      }
    }
  ]
}
```

Example 2 : Autoriser des actions en fonction des balises de ressource

La politique suivante accorde aux utilisateurs l'autorisation d'effectuer des actions et d'obtenir des informations sur les ressources dans CodeConnections.

Pour ce faire, elle autorise des actions spécifiques si le pipeline a une balise nommée `Project` avec la valeur `ProjectA`. (La clé de condition `aws:RequestTag` est utilisée pour contrôler les balises qui

peuvent être transmises dans une demande IAM.) La condition `aws:TagKeys` garantit que la clé de balise est sensible à la casse.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "codestar-connections:CreateConnection",
        "codestar-connections:DeleteConnection",
        "codestar-connections:ListConnections"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/Project": "ProjectA"
        },
        "ForAllValues:StringEquals": {
          "aws:TagKeys": ["Project"]
        }
      }
    }
  ]
}
```

Utilisation de notifications et de connexions dans la console

L'expérience des notifications est intégrée aux CodePipeline consoles CodeBuild, CodeCommit, et CodeDeploy, ainsi que dans la console des outils de développement, dans la barre de navigation des paramètres elle-même. Pour accéder aux notifications dans les consoles, vous devez appliquer l'une des stratégies gérées pour ces services ou disposer d'un ensemble minimal d'autorisations. Ces autorisations doivent vous permettre de répertorier et d'afficher les détails relatifs aux ressources de AWS CodeStar notifications et de AWS CodeStar connexions de votre AWS compte. Si vous créez une politique basée sur l'identité qui est plus restrictive que les autorisations minimales requises, la console ne fonctionnera pas comme prévu pour les entités (utilisateurs et rôles IAM) tributaires de cette politique. Pour plus d'informations sur l'octroi de l'accès à AWS CodeBuild AWS CodeCommit AWS CodeDeploy, AWS CodePipeline, et notamment l'accès à ces consoles, consultez les rubriques suivantes :

- CodeBuild: Utilisation de politiques basées sur l'identité pour CodeBuild

- CodeCommit: Utilisation de politiques basées sur l'identité pour CodeCommit
- AWS CodeDeploy: Gestion des identités et des accès pour AWS CodeDeploy
- CodePipeline: Contrôle d'accès avec des politiques IAM

AWS CodeStar Les notifications ne disposent d'aucune politique AWS gérée. Pour permettre l'accès à la fonction de notification, vous devez soit appliquer l'une des stratégies gérées pour l'un des services répertoriés ci-dessus, soit créer des stratégies avec le niveau d'autorisation que vous souhaitez accorder aux utilisateurs ou aux entités, puis attacher ces stratégies aux utilisateurs, groupes ou rôles qui requièrent ces autorisations. Pour plus d'informations, consultez les exemples suivants :

- Exemple : politique de gestion des notifications au niveau de l'administrateur AWS CodeStar
- Exemple : politique d'utilisation des notifications au niveau des contributeurs AWS CodeStar
- Exemple : read-only-level politique d'utilisation AWS CodeStar des notifications.

AWS CodeStar Connections ne dispose d'aucune politique AWS gérée. Vous utilisez les autorisations et les combinaisons d'autorisations pour l'accès, telles que les autorisations détaillées dans Autorisations pour établir des connexions.

Pour plus d'informations, consultez les ressources suivantes :

- Exemple : politique de gestion au niveau de l'administrateur AWS CodeConnections
- Exemple : politique d'utilisation au niveau du contributeur AWS CodeConnections
- Exemple : read-only-level politique d'utilisation AWS CodeConnections

Il n'est pas nécessaire d'accorder des autorisations de console aux utilisateurs qui appellent uniquement l'API AWS CLI ou l' AWS API. Autorisez plutôt l'accès à uniquement aux actions qui correspondent à l'opération d'API que vous tentez d'effectuer.

Autorisation accordée aux utilisateurs pour afficher leurs propres autorisations

Cet exemple montre comment créer une politique qui permet aux utilisateurs IAM d'afficher les politiques en ligne et gérées attachées à leur identité d'utilisateur. Cette politique inclut les

autorisations permettant d'effectuer cette action sur la console ou par programmation à l'aide de l'API AWS CLI or AWS .

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

Résolution des problèmes liés aux AWS CodeStar notifications et aux AWS CodeStar connexions (identité et accès)

Utilisez les informations suivantes pour identifier et résoudre les problèmes courants que vous pouvez rencontrer lorsque vous travaillez avec les notifications et IAM.

Rubriques

Je suis un administrateur et je veux autoriser d'autres utilisateurs à accéder à des notifications

Pour autoriser d'autres personnes à accéder aux AWS CodeStar notifications et aux AWS CodeStar connexions, vous devez créer une entité IAM (utilisateur ou rôle) pour la personne ou l'application qui doit y accéder. Ils utiliseront les informations d'identification de cette entité pour accéder à AWS. Vous devez ensuite associer une politique à l'entité qui lui accorde les autorisations appropriées dans AWS CodeStar Notifications et AWS CodeStar connexions.

Pour démarrer immédiatement, consultez Création de votre premier groupe et utilisateur délégué IAM dans le Guide de l'utilisateur IAM.

Pour AWS CodeStar des informations spécifiques aux notifications, voirAutorisations et exemples pour les AWS CodeStar notifications.

J'ai créé une rubrique Amazon SNS et l'ai ajoutée en tant que cible de règle de notification, mais je ne reçois pas d'e-mails à propos des événements

Pour recevoir des notifications sur les événements, vous devez disposer d'une rubrique Amazon SNS valide configurée comme cible de la règle de notification et votre adresse e-mail doit être abonnée à la rubrique Amazon SNS. Pour résoudre les problèmes liés à la rubrique Amazon SNS, vérifiez les points suivants :

- Assurez-vous que la rubrique Amazon SNS se trouve dans la même AWS région que la règle de notification.
- Vérifiez que votre alias de messagerie est abonné à la bonne rubrique et que vous avez confirmé l'abonnement. Pour plus d'informations, consultez Abonnement d'un point de terminaison à une rubrique Amazon SNS.

- Vérifiez que la politique du sujet a été modifiée pour autoriser AWS CodeStar les notifications à envoyer des notifications à ce sujet. La stratégie de rubrique doit inclure une instruction similaire à ce qui suit :

```
{
    "Sid": "AWSCodeStarNotifications_publish",
    "Effect": "Allow",
    "Principal": {
        "Service": [
            "codestar-notifications.amazonaws.com"
        ]
    },
    "Action": "SNS:Publish",
    "Resource": "arn:aws:sns:us-east-1:123456789012:MyNotificationTopicName",
    "Condition": {
        "StringEquals": {
            "aws:SourceAccount": "123456789012"
        }
    }
}
```

  Pour plus d'informations, consultez Configuration.

Je souhaite autoriser des personnes extérieures à mon AWS compte à accéder à mes ressources de AWS CodeStar notifications et de AWS CodeStar connexions

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

Pour en savoir plus, consultez les éléments suivants :

- Pour savoir si AWS CodeStar Notifications et AWS CodeStar connexions prend en charge ces fonctionnalités, consultezFonctionnement des fonctions de la console des outils pour développeurs avec IAM.

- Pour savoir comment fournir l'accès à vos ressources sur celles Comptes AWS que vous possédez, consultez la section Fournir l'accès à un utilisateur IAM dans un autre utilisateur Compte AWS que vous possédez dans le Guide de l'utilisateur IAM.
- Pour savoir comment fournir l'accès à vos ressources à des tiers Comptes AWS, consultez la section Fournir un accès à des ressources Comptes AWS détenues par des tiers dans le guide de l'utilisateur IAM.
- Pour savoir comment fournir un accès par le biais de la fédération d'identité, consultez Fournir un accès à des utilisateurs authentifiés en externe (fédération d'identité) dans le Guide de l'utilisateur IAM.
- Pour découvrir quelle est la différence entre l'utilisation des rôles et l'utilisation des politiques basées sur les ressources pour l'accès intercompte, consultez Différence entre les rôles IAM et les politiques basées sur les ressources dans le Guide de l'utilisateur IAM.

Utilisation de rôles liés à un service pour AWS CodeStar Notifications

AWS CodeStar Notifications utilise des rôles liés à un service AWS Identity and Access Management (IAM). Un rôle lié à un service est un type unique de rôle IAM lié directement à AWS CodeStar Notifications. Les rôles liés à un service sont prédéfinis par AWS CodeStar Notifications et comprennent toutes les autorisations nécessaires au service pour appeler d'autres services AWS en votre nom. Ce rôle est créé automatiquement la première fois que vous créez une règle de notification. Vous n'avez donc pas à créer le rôle.

Un rôle lié à un service simplifie la configuration de AWS CodeStar Notifications, car vous n'avez pas besoin d'ajouter manuellement des autorisations. AWS CodeStar Notifications définit les autorisations de ses rôles liés à un service ; sauf définition contraire, seul AWS CodeStar Notifications peut endosser ses rôles. Les autorisations définies comprennent la politique d'approbation et la politique d'autorisation. De plus, cette politique d'autorisation ne peut pas être attachée à une autre entité IAM.

Pour supprimer un rôle lié à un service, vous devez d'abord supprimer ses ressources associées. Vos ressources AWS CodeStar Notifications sont ainsi protégées, car vous ne pouvez pas involontairement supprimer l'autorisation d'accéder aux ressources.

Pour obtenir des informations sur les autres services qui prennent en charge les rôles liés à un service, consultez Services AWS qui fonctionnent avec IAM.

Autorisations de rôle lié à un service pour AWS CodeStar Notifications

AWS CodeStar Notifications utilise le rôle lié au service AWSServiceRoleForCodeStarNotifications pour récupérer des informations sur les événements qui se produisent dans votre chaîne d'outils et envoyer des notifications aux cibles que vous spécifiez.

Le rôle lié au service AWSServiceRoleForCodeStarNotifications approuve les services suivants pour assumer le rôle :

- `codestar-notifications.amazonaws.com`

La stratégie d'autorisations liée au rôle permet à AWS CodeStar Notifications d'exécuter les actions suivantes sur les ressources spécifiées :

- Action : `PutRule` sur `CloudWatch Event rules that are named awscodestar-notifications-*`
- Action : `DescribeRule` sur `CloudWatch Event rules that are named awscodestar-notifications-*`
- Action : `PutTargets` sur `CloudWatch Event rules that are named awscodestar-notifications-*`
- Action : `CreateTopic` sur `create Amazon SNS topics for use with AWS CodeStar Notifications with the prefix CodeStarNotifications-`
- Action : `GetCommentsForPullRequests` sur `all comments on all pull requests in all CodeCommit repositories in the AWS account`
- Action : `GetCommentsForComparedCommit` sur `all comments on all commits in all CodeCommit repositories in the AWS account`
- Action : `GetDifferences` sur `all commits in all CodeCommit repositories in the AWS account`
- Action : `GetCommentsForComparedCommit` sur `all comments on all commits in all CodeCommit repositories in the AWS account`
- Action : `GetDifferences` sur `all commits in all CodeCommit repositories in the AWS account`
- Action : `DescribeSlackChannelConfigurations` sur `all AWS Chatbot clients in the AWS account`

- Action : `UpdateSlackChannelConfiguration` sur `all AWS Chatbot clients in the AWS account`
- Action : `ListActionExecutions` sur `all actions in all pipelines in the AWS account`
- Action : `GetFile` sur `all files in all CodeCommit repositories in the AWS account unless otherwise tagged`

Vous pouvez voir les actions suivantes dans la déclaration de stratégie du rôle lié au service AWSServiceRoleForCodeStarNotifications.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "events:PutTargets",
                "events:PutRule",
                "events:DescribeRule"
            ],
            "Resource": "arn:aws:events:*:*:rule/awscodestarnotifications-*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "sns:CreateTopic"
            ],
            "Resource": "arn:aws:sns:*:*:CodeStarNotifications-*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "codecommit:GetCommentsForPullRequest",
                "codecommit:GetCommentsForComparedCommit",
                "codecommit:GetDifferences",
                "chatbot:DescribeSlackChannelConfigurations",
                "chatbot:UpdateSlackChannelConfiguration",
                "codepipeline:ListActionExecutions"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
```

```
        {
            "Action": [
                "codecommit:GetFile"
            ],
            "Resource": "*",
            "Condition": {
                "StringNotEquals": {
                    "aws:ResourceTag/ExcludeFileContentFromNotifications": "true"
                }
            },
            "Effect": "Allow"
        }
    ]
}
```

Vous devez configurer les autorisations de manière à permettre à une entité IAM (comme un utilisateur, un groupe ou un rôle) de créer, modifier ou supprimer un rôle lié à un service. Pour plus d'informations, consultez Autorisations du rôle lié à un service dans le Guide de l'utilisateur IAM.

Création d'un rôle lié à un service pour AWS CodeStar Notifications

Vous n'avez pas besoin de créer manuellement un rôle lié à un service. Vous pouvez utiliser la console Outils pour développeurs ou l'API CreateNotificationRule à partir de ou des kits SDK pour créer une règle de notification. Vous pouvez également appeler directement l'API. Quelle que soit la méthode que vous utilisez, le rôle lié au service est créé pour vous.

Si vous supprimez ce rôle lié à un service et que vous avez ensuite besoin de le recréer, vous pouvez utiliser la même procédure pour recréer le rôle dans votre compte. Vous pouvez utiliser la console Outils pour développeurs ou l'API CreateNotificationRule à partir de ou des kits SDK pour créer une règle de notification. Vous pouvez également appeler directement l'API. Quelle que soit la méthode que vous utilisez, le rôle lié au service est créé pour vous.

Modification d'un rôle lié à un service pour AWS CodeStar Notifications

Une fois que vous avez créé un rôle lié à un service, vous ne pouvez pas modifier le nom du rôle, car plusieurs entités peuvent faire référence à ce rôle. Néanmoins, vous pouvez utiliser IAM pour modifier la description du rôle. Pour plus d'informations, consultez Modification d'un rôle lié à un service dans le Guide de l'utilisateur IAM.

Suppression d'un rôle lié à un service pour AWS CodeStar Notifications

Si vous n'avez plus besoin d'utiliser une fonction ou un service qui nécessite un rôle lié à un service, nous vous recommandons de supprimer ce rôle. De cette façon, vous n'avez aucune entité inutilisée qui n'est pas surveillée ou gérée activement. Vous devez nettoyer les ressources de votre rôle lié à un service avant de pouvoir les supprimer manuellement. Pour AWS CodeStar Notifications, cela implique de supprimer toutes les règles de notification qui utilisent la fonction du service dans votre compte AWS.

> **Note**
>
> Si le service AWS CodeStar Notifications utilise le rôle lorsque vous essayez de supprimer les ressources, la suppression peut échouer. Si cela se produit, patientez quelques minutes et réessayez.

Pour supprimer les ressources AWS CodeStar Notifications utilisées par AWSServiceRoleForCodeTarNotifications

1. Ouvrez la console Outils pour développeurs AWS à l'adresse https://console.aws.amazon.com/codesuite/settings/notifications.

   > **Note**
   >
   > Les règles de notification sont spécifiques à la région AWS dans laquelle elles sont créées. Si vous disposez de règles de notification dans plusieurs régions AWS, utilisez le sélecteur de région pour modifier la Région AWS.

2. Choisissez toutes les règles de notification qui apparaissent dans la liste, puis choisissez Delete (Supprimer).
3. Répétez ces étapes dans toutes les régions AWS où vous avez créé des règles de notification.

Pour utiliser IAM et supprimer le rôle lié à un service

Utilisez la console IAM, la AWS CLI ou l'API AWS Identity and Access Management pour supprimer le rôle lié au service AWSServiceRoleForCodeStarNotifications. Pour plus d'informations, veuillez consulter Suppression d'un rôle lié à un service dans le Guide de l'utilisateur IAM.

Régions prises en charge pour les rôles liés à un service AWS CodeStar Notifications

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

Utilisation des rôles liés aux services pour AWS CodeConnections

AWS CodeConnections utilise des rôles AWS Identity and Access Management (IAM) liés à un service. Un rôle lié à un service est un type unique de rôle IAM lié directement à AWS CodeConnections. Les rôles liés à un service sont prédéfinis par AWS CodeConnections et comprennent toutes les autorisations nécessaires au service pour appeler d'autres services AWS en votre nom. Ce rôle est créé pour vous la première fois que vous créez une connexion. Vous n'avez donc pas à créer le rôle.

Un rôle lié à un service permet d'utiliser AWS CodeConnections plus facilement, car vous n'avez pas besoin d'ajouter manuellement les autorisations requises. AWS CodeConnections définit les autorisations de ses rôles liés à un service et, sauf définition contraire, seul AWS CodeConnections peut endosser ses rôles. Les autorisations définies comprennent la politique d'approbation et la politique d'autorisation. De plus, cette politique d'autorisation ne peut pas être attachée à une autre entité IAM.

Pour supprimer un rôle lié à un service, vous devez d'abord supprimer ses ressources associées. Vos ressources AWS CodeConnections sont ainsi protégées, car vous ne pouvez pas involontairement supprimer l'autorisation d'accéder aux ressources.

Pour obtenir des informations sur les autres services qui prennent en charge les rôles liés à un service, consultez Services AWS qui fonctionnent avec IAM.

Autorisations des rôles liés à un service pour AWS CodeConnections

AWS CodeConnections utilise le rôle lié à un service AWSServiceRoleForGitSync pour utiliser la synchronisation Git avec les référentiels basés sur Git connectés.

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

- `repository.sync.codeconnections.amazonaws.com`

La politique d'autorisations de rôle nommée AWSGitSyncServiceRolePolicy permet à AWS CodeConnections d'effectuer les actions suivantes sur les ressources spécifiées :

- Action : accorde des autorisations permettant aux utilisateurs de créer des connexions vers des référentiels basés sur Git externes et d'utiliser la synchronisation Git avec ces référentiels.

Vous devez configurer les autorisations de manière à permettre à une entité IAM (comme un utilisateur, un groupe ou un rôle) de créer, modifier ou supprimer un rôle lié à un service. Pour plus d'informations, consultez Autorisations du rôle lié à un service dans le Guide de l'utilisateur IAM.

Création d'un rôle lié à un service pour AWS CodeConnections

Vous n'avez pas besoin de créer manuellement un rôle lié à un service. Vous créez le rôle lorsque vous créez une ressource pour votre projet synchronisé avec Git à l'aide de l'API CreateRepositoryLink.

Si vous supprimez ce rôle lié à un service et que vous avez ensuite besoin de le recréer, vous pouvez utiliser la même procédure pour recréer le rôle dans votre compte.

Modification d'un rôle lié à un service pour AWS CodeConnections

Une fois que vous avez créé un rôle lié à un service, vous ne pouvez pas modifier le nom du rôle, car plusieurs entités peuvent faire référence à ce rôle. Néanmoins, vous pouvez utiliser IAM pour modifier la description du rôle. Pour plus d'informations, consultez Modification d'un rôle lié à un service dans le Guide de l'utilisateur IAM.

Suppression d'un rôle lié à un service pour AWS CodeConnections

Si vous n'avez plus besoin d'utiliser une fonction ou un service qui nécessite un rôle lié à un service, nous vous recommandons de supprimer ce rôle. De cette façon, vous n'avez aucune entité inutilisée qui n'est pas surveillée ou gérée activement. Vous devez nettoyer les ressources de votre rôle lié à un service avant de pouvoir les supprimer manuellement. Cela implique de supprimer toutes les connexions qui utilisent la fonction du service dans votre compte AWS.

> **Note**
>
> Si le service AWS CodeConnections utilise le rôle lorsque vous essayez de supprimer les ressources, la suppression peut échouer. Si cela se produit, patientez quelques minutes et réessayez.

Pour supprimer les ressources AWS CodeConnections utilisées par AWSServiceRoleForGitSync

1. Ouvrez la console Developer Tools, puis choisissez Paramètres.
2. Choisissez toutes connexions qui apparaissent dans la liste, puis Supprimer.
3. Répétez ces étapes dans toutes les régions AWS où vous avez créé des connexions.

Pour utiliser IAM et supprimer le rôle lié à un service

Utilisez la console IAM, l'AWS CLI ou l'API AWS Identity and Access Management pour supprimer le rôle lié au service AWSServiceRoleForGitSync. Pour plus d'informations, veuillez consulter Suppression d'un rôle lié à un service dans le Guide de l'utilisateur IAM.

Régions prises en charge pour les rôles liés à un service AWS CodeConnections

AWS CodeConnections prend en charge l'utilisation des rôles liés à un service dans toutes les régions AWS où le service est disponible. Pour plus d'informations, consultez Régions et Points de terminaison AWS.

Politiques AWS gérées pour AWS CodeConnections

Une politique gérée par AWS est une politique autonome créée et administrée par AWS. Les politiques gérées par AWS 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.

Gardez à l'esprit que les politiques gérées par AWS peuvent ne pas accorder les autorisations de moindre privilège pour vos cas d'utilisation spécifiques, car elles sont disponibles pour tous les clients AWS. 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 stratégies gérées par AWS. Si AWS met à jour les autorisations définies dans une politique gérée par AWS, la mise à jour affecte toutes les identités de principal (utilisateurs, groupes et rôles) auxquelles la politique est associée. AWS est plus susceptible de mettre à jour une politique gérée par AWS lorsqu'un nouveau Service AWS est lancé ou que de nouvelles opérations API deviennent accessibles pour les services existants.

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

Politique gérée par AWS : AWSGitSyncServiceRolePolicy

Vous ne pouvez pas attacher AWSGitSyncServiceRolePolicy à vos entités IAM. Cette politique est attachée à un rôle lié au service qui permet à AWS CodeConnections d'effectuer des actions en votre nom. Pour de plus amples informations, veuillez consulter Utilisation des rôles liés aux services pour AWS CodeConnections.

Cette politique permet aux clients d'accéder à des référentiels basés sur Git à utiliser avec des connexions. Les clients auront accès à ces ressources après avoir utilisé l'API CreateRepositoryLink.

Détails de l'autorisation

Cette politique inclut les autorisations suivantes.

- `codestar-connections` : accorde des autorisations permettant aux utilisateurs de créer des connexions à des référentiels externes basés sur Git.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "AccessGitRepos",
   "Effect": "Allow",
   "Action": [
    "codestar-connections:UseConnection"
   ],
   "Resource": "arn:aws:codestar-connections:*:*:connection/*",
   "Condition": {
    "StringEquals": {
     "aws:ResourceAccount": "${aws:PrincipalAccount}"
    }
```

```
    }
   }
  ]
}
```

Mises à jour AWS CodeConnections vers des politiques gérées par AWS

Consultez le détail des mises à jour des politiques gérées par AWS pour AWS CodeConnections depuis que ce service a commencé à suivre ces modifications. Pour obtenir des alertes automatiques concernant les modifications apportées à cette page, abonnez-vous au flux RSS sur la Page d'historique du document AWS CodeConnections.

Modification	Description	Date
AWSGitSyncServiceRolePolicy : nouvelle politique	AWS CodeConnections a ajouté la politique. Accorde des autorisations permettant aux utilisateurs d'AWS CodeConnections d'utiliser la synchronisation Git avec des référentiels basés sur Git connectés.	26 novembre 2023
AWS CodeConnections a démarré le suivi des modifications	AWS CodeConnections a commencé à suivre les modifications pour ses politiques gérées par AWS.	26 novembre 2023

Validation de conformité pour AWS CodeStar les notifications et AWS CodeStar les connexions

AWS CodeStar Les notifications et les AWS CodeStar connexions ne sont couvertes par aucun programme de AWS conformité.

Pour une liste des AWS services concernés par des programmes de conformité spécifiques, voir AWS Services concernés par programme de conformité. Pour obtenir des informations générales, veuillez consulter Programmes de conformité d'AWS.

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

Lorsque vous utilisez AWS CodeStar Notifications et AWS CodeStar connexions, votre responsabilité en matière de conformité dépend de la sensibilité de vos données, des objectifs de conformité de votre entreprise et des lois et réglementations applicables. AWS fournit les ressources suivantes pour faciliter la mise en conformité :

- Guides de démarrage rapide sur la sécurité et la conformité : ces guides de déploiement abordent les considérations architecturales et indiquent les étapes à suivre pour déployer des environnements de base axés sur la sécurité et la conformité sur. AWS
- AWS ressources relatives à la conformité : cette collection de classeurs et de guides peut s'appliquer à votre secteur d'activité et à votre région.
- AWS Config— Ce AWS service évalue dans quelle mesure les configurations de vos ressources sont conformes aux pratiques internes, aux directives du secteur et aux réglementations.
- AWS Security Hub— Ce AWS service fournit une vue complète de l'état de votre sécurité interne, AWS ce qui vous permet de vérifier votre conformité aux normes et aux meilleures pratiques du secteur de la sécurité.

Résilience dans AWS CodeStar Notifications et AWS CodeStar Connections

L'infrastructure mondiale d'AWS s'articule autours de régions et de zones de disponibilité AWS. AWS Les Régions fournissent plusieurs zones de disponibilité physiquement séparées et isolées, reliées par un réseau à latence faible, à haut débit et hautement redondant. Avec les zones de disponibilité, vous pouvez concevoir et exploiter des applications et des bases de données qui basculent automatiquement d'une zone de disponibilité à l'autre sans interruption. Les zones de disponibilité sont plus hautement disponibles, tolérantes aux pannes et évolutives que les infrastructures traditionnelles à un ou plusieurs centres de données.

Pour plus d'informations sur les régions AWS et les zones de disponibilité, veuillez consulter Infrastructure mondiale AWS.

- Les règles de notification sont spécifiques à la Région AWS dans laquelle elles sont créées. Si vous disposez de règles de notification dans plusieurs Région AWS, utilisez le sélecteur de région pour consulter les règles de notification dans chaque Région AWS.
- AWS CodeStar Notifications s'appuie sur les rubriques Amazon Simple Notification Service (Amazon SNS) comme cibles de règle de notification. De ce fait, les informations sur vos rubriques Amazon SNS et les cibles de règle de notification peuvent être stockées dans une région AWS en dehors de la région où vous avez configuré la règle de notification.

Sécurité de l'infrastructure dans AWS CodeStar Notifications et AWS CodeStar Connections

En tant que fonctions d'un service géré, AWS CodeStar Notifications et AWS CodeStar Connections sont protégés par les procédures de sécurité du réseau mondial AWS décrites dans le livre blanc Amazon Web Services : Présentation des procédures de sécurité.

Vous utilisez les appels d'API AWS publiés pour accéder à AWSCodeStar Notifications et AWS CodeStar Connections via le réseau. Les clients doivent supporter le protocole TLS (Sécurité de la couche transport) 1.0 ou une version ultérieure. Les clients doivent aussi prendre en charge les suites de chiffrement PFS (Perfect Forward Secrecy) comme Ephemeral Diffie-Hellman (DHE) ou Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). La plupart des systèmes modernes prennent en charge ces modes.

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

Trafic entre les ressources AWS CodeConnections entre régions

Si vous utilisez la fonction de connexion pour activer la connexion de vos ressources, vous acceptez et nous demandez de stocker et de traiter les informations associées à ces ressources de connexion dans les Régions AWS en dehors des Régions AWS où vous utilisez le service sous-jacent dans le seul but de fournir une connexion avec ces ressources dans des régions autres que celle où la ressource a été créée.

Pour de plus amples informations, veuillez consulter Ressources mondiales dans AWS CodeStar Connections.

> **Note**
>
> Si vous utilisez la fonction de connexions pour activer la connexion à vos ressources dans des régions qui ne nécessitent pas d'être activées au préalable, nous stockons et traitons les informations comme indiqué dans les rubriques précédentes.
> Pour les connexions établies dans des régions qui doivent d'abord être activées, telles que la région Europe (Milan), nous stockons et traitons uniquement les informations relatives à cette connexion dans cette région.

Historique du document

Le tableau suivant décrit la documentation de cette version de la console Outils pour développeurs.

- Version de l'API AWS CodeStar Notifications : 15-10-2019
- Version de l'API AWS CodeStar Connections : 01-12-2019

Modification	Description	Date
Prise en charge de GitLab autogéré	Ajout de la prise en charge de la configuration des connexions et des hôtes afin de permettre aux ressources AWS d'interagir avec GitLab autogéré. Pour plus d'informations, consultez Flux de travail de création ou de mise à jour d'un hôte et Création d'une connexion à GitLab autogéré.	28 décembre 2023
Nouveaux liens de référentiel et nouvelles configurations de synchronisation pour les connexions	Ajout d'informations sur la configuration des liens de référentiel et des configurations de synchronisation. Utilisez la configuration de synchronisation pour synchroniser le contenu d'un référentiel Git afin de mettre à jour les ressources de votre pile AWS CloudFormation. Pour plus d'informations, consultez Utilisation des liens de référentiel et Utilisation des configurations de synchronisation.	27 novembre 2023

Prise en charge des connexions service-linked-role	Prise en charge ajoutée pour configurer les connexions afin d'utiliser la synchronisation Git avec les référentiels Git. Pour plus d'informations, consultez Utilisation des rôles liés à un service pour les connexions AWS CodeStar et Politiques gérées.	26 novembre 2023
Prise en charge des groupes GitLab	Ajout de la prise en charge pour configurer les connexions permettant aux ressources AWS d'interagir avec les groupes GitLab. Pour plus d'informations, consultez Création d'une connexion et Création d'une connexion à GitLab.	15 septembre 2023
Nouveau type de fournisseur GitLab	Vous pouvez désormais créer des connexions à GitLab. Pour plus d'informations, consultez Création d'une connexion et Création d'une connexion à GitLab.	10 août 2023

Nouveau type de cible pour les règles de notification	Vous pouvez désormais choisir des clients AWS Chatbot configurés pour les canaux Microsoft Teams comme cibles des règles de notification. Pour de plus amples informations, veuillez consulter Création d'une règle de notification et Utilisation des cibles de règle de notification.	17 mai 2023
Des connexions sont disponibles dans la région Europe (Milan)	Informations supplémentaires pour les connexions dans la région Europe (Milan). Pour plus d'informations, consultez Trafic entre les ressources AWS CodeStar Connections d'une région à l'autre.	17 mai 2023
Ajout du dépannage pour les erreurs de connexion avec les autorisations du référentiel	Lorsque vous créez une connexion à un référentiel dans une organisation GitHub, vous devez être le propriétaire de cette dernière. Pour plus d'informations, veuillez consulter la rubrique Erreur de connexion lors de la connexion à GitHub.	29 août 2022
Ajout d'informations pour le balisage des ressources hôtes	Vous pouvez désormais étiqueter les hôtes à l'aide de la console et de la CLI. Pour de plus amples informations, veuillez consulter Baliser des ressources dans AWS CodeStar Connections.	19 avril 2021

Prise en charge des points de terminaison d'un VPC pour les connexions	Vous pouvez utiliser les points de terminaison d'un VPC avec des connexions. Pour de plus amples informations, veuillez consulter AWS CodeStar Connections et les points de terminaison de VPC d'interface (AWS PrivateLink).	24 novembre 2020
Types de fournisseurs pris en charge pour GitHub et GitHub Enterprise Cloud	Vous pouvez désormais créer des connexions à GitHub et GitHub Enterprise Cloud. Pour de plus amples informations, veuillez consulter Créer une connexion et Créer une connexion à GitHub.	30 septembre 2020
Ajout du type de fournisseur GitHub Enterprise Server et des ressources hôtes	Des informations sur la ressource hôte pour les connexions ont été ajoutées à ce guide. Vous pouvez désormais créer des connexions à GitHub Enterprise Server Pour de plus amples informations, veuillez consulter Créer une connexion et Travailler avec des hôtes. Voici la version générale de la fonction Connexions dans le guide de l'utilisateur de la console Outils pour développeurs.	29 juin 2020

Ajout d'informations pour l'utilisation et le balisage des connexions	Des informations sur la fonction de connexion de la console ont été ajoutées à ce guide. Vous pouvez afficher les concepts, les étapes de démarrage, une référence des autorisations, y compris des exemples de politiques et les étapes pour créer, afficher et étiqueter les connexions. Pour de plus amples informations, veuillez consulter Que sont les connexions, Concepts de connexions, Premiers pas avec les connexions, Créer une connexion,Étiqueter des ressources dans AWS CodeStar Connections, Sécurité, Quotas pour les connexions, Résolution des problèmes et Appels API AWS CodeStar Connections avec AWS CloudTrail. Pour afficher la liste des actions supplémentaires du fournisseur (actions d'autorisations uniquement), consultez Actions pour ProviderType.	28 juin 2020

Nouveau type de cible pour les règles de notification	Vous pouvez désormais choisir des clients AWS Chatbot configurés pour les canaux Slack comme cibles des règles de notification. Pour de plus amples informations, veuillez consulter Création d'une règle de notification et Utilisation des cibles de règle de notification.	2 avril 2020
Ajout de notifications sur les événements AWS CodeCommit supplémentaires	Vous pouvez désormais configurer des notifications pour les événements liés aux approbations de demande d'extraction. Pour de plus amples informations, veuillez consulter Événements pour les règles de notification pour les référentiels et Utilisation des demandes d'extraction dans CodeCommit.	10 février 2020
Notifications disponibles dans deux régions AWS supplémentaires	La console Outils pour développeurs prend désormais en charge les notifications au Moyen-Orient (Bahreïn) et en Asie-Pacifique (Hong Kong). Pour de plus amples informations, veuillez consulter Notifications CodeStar AWS dans le Références générales AWS.	5 février 2020

Ajout de la prise en charge des rubriques Amazon SNS chiffrées	Des conseils ont été ajoutés pour utiliser les rubriques Amazon SNS chiffrées comme cibles de notification. Pour plus d'informations, consultez Configuration des rubriques Amazon SNS pour les notifications .	4 février 2020
Les notifications peuvent inclure des informations de balise de session pour CodeCommit	Les notifications pour CodeCommit peuvent désormais contenir des informations sur l'identité de l'utilisateur, telles qu'un nom complet ou une adresse e-mail, grâce à l'utilisation de balises de session. Pour plus d'informations, consultez Concepts et Utilisation de balises pour fournir des informations d'identité dans CodeCommit.	19 décembre 2019
Première version	Il s'agit de la première version de la console Outils pour développeurs et du guide de l'utilisateur.	5 novembre 2019

Glossaire AWS

Pour connaître la terminologie la plus récente d'AWS, consultez le Glossaire AWS dans la Référence Glossaire AWS.

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.