



Guide de l'utilisateur

AWS CodeStar



AWS CodeStar: Guide de l'utilisateur

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

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

Table of Contents

.....	viii
Qu'est-ce qu'AWS CodeStar ?	1
Que puis-je faire avec AWS CodeStar ?	1
Comment démarrer avec AWS CodeStar ?	2
Configuration	3
Étape 1 : Créer un compte	3
Inscrivez-vous pour un Compte AWS	3
Création d'un utilisateur doté d'un accès administratif	4
Étape 2 : créer le rôle AWS CodeStar de service	5
Étape 3 : Configurer les autorisations IAM de l'utilisateur	5
Étape 4 : Création d'une paire de clés Amazon EC2 pour les projets AWS CodeStar	6
Étape 5 : ouvrir la AWS CodeStar console	6
Étapes suivantes	7
Démarrer avec AWS CodeStar	8
Étape 1 : Créer un projet AWS CodeStar	9
Étape 2 : ajouter des informations d'affichage pour votre profil AWS CodeStar utilisateur	14
Étape 3 : Afficher votre projet	15
Étape 4 : valider une modification	16
Étape 5 : Ajouter d'autres membres à l'équipe	21
Étape 6 : Nettoyage	24
Étape 7 : Préparez votre projet pour un environnement de production	25
Étapes suivantes	25
Didacticiel sur les projets sans serveur	25
Présentation	26
Étape 1 : création du projet	27
Étape 2 : Parcourir les ressources du projet	29
Étape 3 : Tester le service web	32
Étape 4 : Configurer votre poste de travail local pour modifier le code du projet	33
Étape 5 : Ajouter la logique au service web	33
Étape 6 : Tester le service web amélioré	36
Étape 7 : Ajouter un test unitaire pour le service web	37
Étape 8 : Afficher les résultats du test unitaire	39
Étape 9 : Nettoyer	40
Étapes suivantes	41

Didacticiel du projet d'AWS CLI	41
Étape 1 : Téléchargement et examen de l'exemple de code source	42
Étape 2 : Téléchargement de l'exemple de modèle de chaîne d'outils	43
Étape 3 : Test de votre modèle de chaîne d'outils dans AWS CloudFormation	44
Étape 4 : Chargement de votre code source et de votre modèle de chaîne d'outils	45
Étape 5 : Création d'un projet dans AWS CodeStar	46
Didacticiel sur un projet de compétence Alexa	49
Prérequis	49
Étape 1 : Créer le projet et vous connecter à votre compte de développeur Amazon	50
Étape 2 : Tester votre compétence dans le simulateur Alexa	51
Étape 3 : Parcourir les ressources du projet	52
Étape 4 : Modifier la réponse de votre compétence	52
Étape 5 : Configurer votre poste de travail local pour qu'il se connecte à votre référentiel de projet	53
Étapes suivantes	53
Tutoriel : Création d'un projet avec un référentiel GitHub source	54
Étape 1 : Création du projet et création de votre GitHub référentiel	54
Étape 2 : Afficher votre code source	58
Étape 3 : créer une GitHub pull request	58
Modèles de projet	60
Fichiers et ressources de projet AWS CodeStar	60
Mise en route : Choix d'un modèle de projet	62
Choix d'une plateforme de calcul de modèle	62
Choix d'un type d'application de modèle	63
Choix d'un langage de programmation de modèle	64
Comment procéder pour modifier votre projet AWS CodeStar	64
Modification du code source de l'application et transmission des modifications	65
Modifier les ressources de l'application à l'aide du fichier Template.yml	65
.....	66
Bonnes pratiques AWS CodeStar	67
Bonnes pratiques de sécurité pour les ressources AWS CodeStar	67
Bonnes pratiques en matière de définition des versions de dépendances	67
Surveillance et journalisation des bonnes pratiques pour les ressources AWS CodeStar	68
Utilisation des projets	69
Créer un projet	71
Créer un projet dans AWS CodeStar (Console)	71

Créer un projet dans AWS CodeStar (AWS CLI)	76
Utilisation d'un IDE avec AWS CodeStar	83
Utiliser AWS Cloud9 avec AWS CodeStar	84
Utilisation d'Eclipse avec AWS CodeStar	92
Utilisez Visual Studio avec AWS CodeStar	97
Modifier les ressources d'un projet	99
Modifications des ressources prises en charge	99
Ajouter une étape à AWS CodePipeline	101
Modifier des paramètres de l'environnement AWS Elastic Beanstalk	101
Modifier une fonction AWS Lambda dans le code source	102
Activer le suivi d'un projet	102
Ajout d'une ressource à un projet	105
Ajoutez un rôle IAM à un projet	111
Ajoutez une étape de prod et un point de terminaison à un projet	112
Utiliser les paramètres SSM en toute sécurité dans un projet AWS CodeStar	121
Déplacer le trafic pour un projet AWS Lambda	123
Transition de votre projet AWS CodeStar vers la production	130
Création d'un référentiel GitHub	131
Utilisation des balises de projet	132
Ajout d'une balise à un projet	133
Suppression d'une balise d'un projet	133
Obtention de la liste de balises d'un projet	133
Supprimer un projet	134
Supprimer un projet dans AWS CodeStar (console)	135
Supprimer un projet dans AWS CodeStar (AWS CLI)	136
Utilisation des équipes	138
Ajouter des membres de l'équipe à un projet	140
Ajouter un membre d'équipe (Console)	142
Ajouter et afficher des membres de l'équipe (AWS CLI)	144
Gérer les autorisations de l'équipe	145
Gérer les autorisations de l'équipe (Console)	146
Gérer les autorisations de l'équipe (AWS CLI)	147
Supprimer des membres d'une équipe dans un projet	147
Supprimer des membres de l'équipe (Console)	148
Supprimer des membre de l'équipe (AWS CLI)	149
Utilisation de votre profil utilisateur AWS CodeStar	150

Gérer les informations d'affichage	150
Gérer votre profil utilisateur (Console)	151
Gérer les profils utilisateur (AWS CLI)	152
Ajouter une clé publique à votre profil utilisateur	155
Gérer votre clé publique (console)	155
Gérer votre clé publique (AWS CLI)	156
Connectez-vous à une instance Amazon EC2 avec votre clé privée	157
Sécurité	159
Protection des données	160
Chiffrement des données dans AWS CodeStar	161
Gestion de l'identité et des accès	161
Public ciblé	162
Authentification avec des identités	162
Gestion des accès à l'aide de politiques	166
Comment AWS CodeStar fonctionne avec IAM	169
AWS CodeStar Politiques et autorisations au niveau du projet	180
Exemples de politiques basées sur l'identité	187
Résolution des problèmes	218
Journalisation des AWS CodeStar appels d'API avec AWS CloudTrail	220
AWS CodeStarInformations dans CloudTrail	221
Présentation des entrées des fichiers journaux AWS CodeStar	222
Validation de la conformité	223
Résilience	224
Sécurité de l'infrastructure	224
Limites	226
Résolution des problèmes AWS CodeStar	228
Échec de création d'un projet : un projet n'a pas été créé	228
Création de projet : une erreur s'affiche lorsque j'essaie de modifier la configuration Amazon EC2 lors de la création d'un projet	229
Suppression de projet : un AWS CodeStar projet a été supprimé, mais les ressources existent toujours	230
Échec de la gestion de l'équipe : impossible d'ajouter un utilisateur IAM à une équipe dans un projet AWS CodeStar	231
Échec d'accès : un utilisateur fédéré ne peut pas accéder à un projet AWS CodeStar	232
Échec d'accès : un utilisateur fédéré ne peut pas accéder à un environnement ou en créer un AWS Cloud9	232

Échec d'accès : un utilisateur fédéré peut créer un AWS CodeStar projet, mais ne peut pas afficher les ressources du projet	233
Problème avec le rôle de service : le rôle de service n'a pas pu être créé	233
Problème lié au rôle de service : le rôle de service n'est pas valide ou est manquant	233
Problème lié au rôle du projet : les vérifications de l'état de AWS Elastic Beanstalk santé échouent pour certaines instances d'un AWS CodeStar projet	234
Problème lié au rôle de projet : un rôle de projet n'est pas valide ou est manquant	235
Extensions de projet : Impossible de se connecter à JIRA	235
GitHub: Impossible d'accéder à l'historique des validations, aux problèmes ou au code d'un dépôt	235
AWS CloudFormation : Création de la pile annulée en raison d'autorisations manquantes	236
AWS CloudFormation n'est pas autorisé à exécuter le rôle d'exécution iam : PassRole on Lambda	236
Impossible de créer la connexion pour un GitHub dépôt	237
Notes de mise à jour	238
Glossaire AWS	244

Le 31 juillet 2024, Amazon Web Services (AWS) cessera de prendre en charge la création et la visualisation de AWS CodeStar projets. Après le 31 juillet 2024, vous ne pourrez plus accéder à la AWS CodeStar console ni créer de nouveaux projets. Toutefois, les AWS ressources créées par AWS CodeStar, y compris vos référentiels sources, vos pipelines et vos versions, ne seront pas affectées par cette modification et continueront de fonctionner. AWS CodeStar Les connexions et AWS CodeStar les notifications ne seront pas affectées par cette interruption.

Si vous souhaitez suivre le travail, développer du code et créer, tester et déployer vos applications, Amazon CodeCatalyst propose un processus de démarrage rationalisé et des fonctionnalités supplémentaires pour gérer vos projets logiciels. En savoir plus sur [les fonctionnalités](#) et [les tarifs](#) d'Amazon CodeCatalyst.

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.

Qu'est-ce qu'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. Un projet AWS CodeStar crée et intègre des services AWS pour votre chaîne d'outils de développement de projet. Selon votre choix de modèle de projet AWS CodeStar, cette chaîne d'outils peut inclure des ressources de contrôle du code source, de génération, de déploiement, avec des serveurs virtuels ou sans serveur, etc. AWS CodeStar gère également les autorisations requises pour les utilisateurs du projet (appelés membres de l'équipe). En ajoutant les utilisateurs en tant que membres de l'équipe à un projet AWS CodeStar, les propriétaires du projet peuvent accorder rapidement et simplement à chaque membre de l'équipe un accès à un projet et à ses ressources qui est conforme à son rôle.

Rubriques

- [Que puis-je faire avec AWS CodeStar ?](#)
- [Comment démarrer avec AWS CodeStar ?](#)

Que puis-je faire avec AWS CodeStar ?

AWS CodeStar vous permet de configurer votre développement d'applications dans le cloud et de le gérer dans un seul tableau de bord centralisé. Plus précisément, vous pouvez :

- Démarrer de nouveaux projets logiciels sur AWS en quelques minutes en utilisant des modèles pour applications web, services web, entre autres : AWS CodeStar inclut des modèles de projet pour différents types de projets et langages de programmation. Dans la mesure où AWS CodeStar s'occupe de la configuration, toutes les ressources du projet sont configurées pour fonctionner ensemble.
- Gérer l'accès au projet pour votre équipe : AWS CodeStar fournit une console centrale où vous pouvez attribuer aux membres de l'équipe de projet les rôles dont ils ont besoin pour accéder aux outils et aux ressources. Ces autorisations sont appliquées automatiquement à tous les AWS services utilisés dans votre projet. Vous n'avez donc pas besoin de créer ou de gérer des politiques IAM complexes.
- Visualiser, gérer et collaborer sur vos projets à un seul endroit : AWS CodeStar comprend un tableau de bord de projet qui fournit une vue d'ensemble du projet, de sa chaîne d'outils et de ses événements importants. Vous pouvez surveiller la dernière activité de projet, par exemple les

validations de code récentes, et suivre l'état de vos modifications de code, générer des résultats et des déploiements, tout cela dans la même page web. Vous pouvez surveiller ce qui se passe dans le projet dans un seul tableau de bord et explorer les problèmes à étudier.

- Itérer rapidement avec tous les outils dont vous avez besoin : AWS CodeStar inclut une chaîne d'outils de développement intégrée pour votre projet. Les membres de l'équipe transmettent du code, et les modifications sont déployées automatiquement. L'intégration avec le suivi des problèmes permet aux membres de l'équipe de suivre ce qu'il faut faire ensuite. Vous et votre équipe pouvez collaborer plus rapidement et efficacement dans toutes les phases de livraison de code.

Comment démarrer avec AWS CodeStar ?

Pour commencer à utiliser AWS CodeStar :

1. Préparez-vous à utiliser AWS CodeStar en suivant les étapes énoncées dans [Configuration AWS CodeStar](#).
2. Essayez AWS CodeStar en suivant les étapes indiquées dans les didacticiels [Démarrer avec AWS CodeStar](#).
3. Partagez votre projet avec d'autres développeurs en suivant les étapes indiquées dans [Ajouter des membres de l'équipe à un projet AWS CodeStar](#).
4. Intégrez votre IDE favori en suivant les étapes indiquées dans [Utilisation d'un IDE avec AWS CodeStar](#).

Configuration AWS CodeStar

Avant de commencer à l'utiliser AWS CodeStar, vous devez suivre les étapes suivantes.

Rubriques

- [Étape 1 : Créer un compte](#)
- [Étape 2 : créer le rôle AWS CodeStar de service](#)
- [Étape 3 : Configurer les autorisations IAM de l'utilisateur](#)
- [Étape 4 : Création d'une paire de clés Amazon EC2 pour les projets AWS CodeStar](#)
- [Étape 5 : ouvrir la AWS CodeStar console](#)
- [Étapes suivantes](#)

Étape 1 : Créer un compte

Inscrivez-vous pour un Compte AWS

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

Pour vous inscrire à un Compte AWS

1. Ouvrez <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 vous inscrivez à un Compte AWS, un Utilisateur racine d'un compte AWS est créé. Par défaut, seul l'utilisateur racine a accès à l'ensemble des Services AWS et des ressources de ce compte. Pour des raisons de sécurité, attribuez un accès administratif à un utilisateur et utilisez uniquement l'utilisateur root pour effectuer [les tâches nécessitant un accès utilisateur root](#).

AWS vous envoie un e-mail de confirmation une fois le processus d'inscription 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 choisissant Mon compte.

Création d'un utilisateur doté d'un accès administratif

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

Sécurisez votre Utilisateur racine d'un compte AWS

1. Connectez-vous en [AWS Management Console](#) tant que propriétaire du compte en choisissant Utilisateur root et en saisissant votre adresse Compte AWS e-mail. Sur la page suivante, saisissez votre mot de passe.

Pour obtenir de l'aide pour vous connecter en utilisant l'utilisateur racine, consultez [Connexion en tant qu'utilisateur racine](#) dans le Guide de l'utilisateur Connexion à AWS .

2. Activez l'authentification multifactorielle (MFA) pour votre utilisateur racine.

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

Création d'un utilisateur doté d'un accès administratif

1. Activez IAM Identity Center.

Pour obtenir des instructions, consultez [Activation d' AWS IAM Identity Center](#) dans le Guide de l'utilisateur AWS IAM Identity Center .

2. Dans IAM Identity Center, accordez un accès administratif à un utilisateur.

Pour un didacticiel sur l'utilisation du Répertoire IAM Identity Center comme source d'identité, voir [Configurer l'accès utilisateur par défaut Répertoire IAM Identity Center](#) dans le Guide de AWS IAM Identity Center l'utilisateur.

Connectez-vous en tant qu'utilisateur disposant d'un accès administratif

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

Pour obtenir de l'aide pour vous connecter en utilisant un utilisateur d'IAM Identity Center, consultez la section [Connexion au portail AWS d'accès](#) dans le guide de l'Connexion à AWS utilisateur.

Attribuer l'accès à des utilisateurs supplémentaires

1. Dans IAM Identity Center, créez un ensemble d'autorisations conforme aux meilleures pratiques en matière d'application des autorisations du moindre privilège.

Pour obtenir des instructions, voir [Création d'un ensemble d'autorisations](#) dans le guide de AWS IAM Identity Center l'utilisateur.

2. Affectez des utilisateurs à un groupe, puis attribuez un accès d'authentification unique au groupe.

Pour obtenir des instructions, voir [Ajouter des groupes](#) dans le guide de AWS IAM Identity Center l'utilisateur.

Étape 2 : créer le rôle AWS CodeStar de service

Créez un [rôle de service](#) utilisé pour AWS CodeStar autoriser l'administration des AWS ressources et des autorisations IAM en votre nom. Vous ne devez créer le rôle de service qu'une seule fois.

Important

Vous devez être connecté en tant qu'utilisateur administratif (ou compte racine) pour créer un rôle de service. Pour plus d'informations, consultez [la section Création de votre premier utilisateur et groupe IAM](#).

1. Ouvrez la AWS CodeStar console à l'[adresse https://console.aws.amazon.com/codestar/](https://console.aws.amazon.com/codestar/).
2. Choisissez Démarrer un projet.

Si vous ne voyez pas l'option Démarrer un projet mais que vous êtes redirigé vers la page de la liste des projets, le rôle de service a été créée.

3. Dans la boîte de dialogue Créer un rôle de service, choisissez Oui, créer le rôle.
4. Quittez l'assistant. Vous y reviendrez ultérieurement.

Étape 3 : Configurer les autorisations IAM de l'utilisateur

Outre l'utilisateur administratif, vous pouvez l'utiliser AWS CodeStar en tant qu'utilisateur IAM, utilisateur fédéré, utilisateur root ou en tant que rôle assumé. Pour plus d'informations sur ce qui

AWS CodeStar peut être fait pour les utilisateurs IAM par rapport aux utilisateurs fédérés, consultez.

[AWS CodeStar IAM Rôles](#)

Si vous n'avez configuré aucun utilisateur IAM, consultez la section Utilisateur [IAM](#).

Pour activer l'accès, ajoutez des autorisations à vos utilisateurs, groupes ou rôles :

- Utilisateurs et groupes dans AWS IAM Identity Center :

Créez un jeu d'autorisations. Suivez les instructions de la rubrique [Création d'un jeu d'autorisations](#) du Guide de l'utilisateur AWS IAM Identity Center .

- Utilisateurs gérés dans IAM par un fournisseur d'identité :

Créez un rôle pour la fédération d'identité. Pour plus d'informations, voir la rubrique [Création d'un rôle pour un fournisseur d'identité tiers \(fédération\)](#) du Guide de l'utilisateur IAM.

- Utilisateurs IAM :

- Créez un rôle que votre utilisateur peut assumer. Suivez les instructions de la rubrique [Création d'un rôle pour un utilisateur IAM](#) du Guide de l'utilisateur IAM.

- (Non recommandé) Attachez une politique directement à un utilisateur ou ajoutez un utilisateur à un groupe d'utilisateurs. Suivez les instructions de la rubrique [Ajout d'autorisations à un utilisateur \(console\)](#) du Guide de l'utilisateur IAM.

Étape 4 : Création d'une paire de clés Amazon EC2 pour les projets AWS CodeStar

De nombreux AWS CodeStar projets utilisent AWS CodeDeploy ou AWS Elastic Beanstalk déploient du code sur des instances Amazon EC2. Pour accéder aux instances Amazon EC2 associées à votre projet, créez une paire de clés Amazon EC2 pour votre utilisateur IAM. Votre utilisateur IAM doit être autorisé à créer et à gérer les clés Amazon EC2 (par exemple, l'autorisation d'effectuer `ec2:CreateKeyPair` les actions `ec2:ImportKeyPair` et). Pour plus d'informations, consultez [Paires de clés Amazon EC2](#).

Étape 5 : ouvrir la AWS CodeStar console

Connectez-vous à la AWS CodeStar console AWS Management Console, puis ouvrez-la à l'adresse <https://console.aws.amazon.com/codestar/>.

Étapes suivantes

Félicitations, vous avez terminé la configuration ! Pour commencer à travailler avec AWS CodeStar, voir [Démarrer avec AWS CodeStar](#).

Démarrer avec AWS CodeStar

Dans ce didacticiel, vous utiliserez AWS CodeStar pour créer une application web. Ce projet inclut un exemple de code dans un référentiel source, une chaîne d'outils de déploiement continu et un tableau de bord de projet où vous pouvez afficher et surveiller votre projet.

En suivant les étapes, vous allez :

- Créer un projet dans AWS CodeStar.
- Explorer ce projet.
- Valider une modification de code.
- Voir votre modification de code se déployer automatiquement.
- Ajouter d'autres personnes qui travailleront sur votre projet.
- Nettoyer les ressources de projet lorsqu'elles ne seront plus nécessaires.

Note

Si vous ne l'avez pas déjà fait, suivez d'abord la procédure présentée dans [Configuration AWS CodeStar](#), notamment [Étape 2 : créer le rôle AWS CodeStar de service](#). Vous devez être connecté avec un compte qui est un utilisateur administratif dans IAM. Pour créer un projet, vous devez vous connecter à l'AWS Management Console aide d'un utilisateur IAM disposant de cette **AWSCodeStarFullAccess** politique.

Rubriques

- [Étape 1 : Créer un projet AWS CodeStar](#)
- [Étape 2 : ajouter des informations d'affichage pour votre profil AWS CodeStar utilisateur](#)
- [Étape 3 : Afficher votre projet](#)
- [Étape 4 : valider une modification](#)
- [Étape 5 : Ajouter d'autres membres à l'équipe](#)
- [Étape 6 : Nettoyage](#)
- [Étape 7 : Préparez votre projet pour un environnement de production](#)

- [Étapes suivantes](#)
- [Didacticiel : Création et gestion d'un projet sans serveur dans AWS CodeStar](#)
- [Didacticiel : Création d'un projet dans AWS CodeStar à l'aide de l'AWS CLI](#)
- [Tutoriel : créer un projet de compétence Alexa dans AWS CodeStar](#)
- [Tutoriel : Création d'un projet avec un référentiel GitHub source](#)

Étape 1 : Créer un projet AWS CodeStar

Au cours de cette étape, vous allez créer un projet de développement logiciel JavaScript (Node.js) pour une application Web. Vous utilisez un modèle de AWS CodeStar projet pour créer le projet.

Note

Le modèle de AWS CodeStar projet utilisé dans ce didacticiel utilise les options suivantes :

- Catégorie d'application : application web
- Langage de programmation : Node.js
- AWSService : Amazon EC2

Si vous choisissez d'autres options, vous obtiendrez des résultats différents de ceux présentés dans ce didacticiel.

Pour créer un projet dans AWS CodeStar

1. Connectez-vous à la AWS CodeStar console AWS Management Console, puis ouvrez-la à l'adresse <https://console.aws.amazon.com/codestar/>.

Vérifiez que vous êtes connecté à la région AWS dans laquelle vous souhaitez créer le projet et ses ressources. Par exemple, pour créer un projet dans l'est des États-Unis (Ohio), assurez-vous d'avoir sélectionné cette AWS région. Pour plus d'informations sur les régions AWS dans lesquelles AWS CodeStar est disponible, consultez [Régions et points de terminaison](#) dans le document Référence générale AWS.

2. Sur la AWS CodeStar page, choisissez Créer un projet.
3. Sur la page Choisir un modèle de projet, choisissez le type de projet dans la liste des modèles de AWS CodeStar projet. Vous pouvez utiliser la barre de filtre pour affiner vos choix. Par


exemple, pour un projet d'application Web écrit dans Node.js à déployer sur des instances Amazon EC2, cochez les cases Application Web, Node.js et Amazon EC2. Ensuite, choisissez parmi les modèles disponibles pour cet ensemble d'options.

Pour plus d'informations, veuillez consulter [Modèles de projet AWS CodeStar](#).

4. Choisissez Suivant.
5. Dans le champ de saisie du nom du projet, entrez un nom pour le projet, tel que *Mon premier projet*. Dans Project ID, l'ID du projet est dérivé du nom du projet, mais il est limité à 15 caractères.

Par exemple, l'ID par défaut d'un projet nommé *Mon premier projet* est *my-first-projec*. Cet identifiant de projet est à la base des noms de toutes les ressources associées au projet. AWS CodeStar utilise cet ID de projet dans l'URL de votre référentiel de code et pour les noms des rôles et politiques d'accès de sécurité associés dans IAM. Une fois le projet créé, l'ID de projet ne peut pas être modifié. Pour modifier l'ID de projet avant de créer le projet, dans ID de projet, entrez l'ID que vous souhaitez utiliser.


Pour plus d'informations sur les limites des noms de projet et des ID de projet, consultez [Limites dans AWS CodeStar](#).

 Note

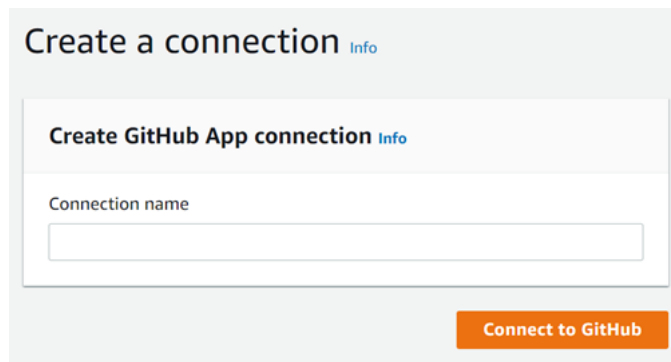
Les ID de projet doivent être uniques pour votre compte AWS dans une région AWS.

6. Choisissez le fournisseur de référentiel, AWS CodeCommit ou GitHub.
7. Si vous avez choisi AWS CodeCommit, dans Nom du référentiel, acceptez le nom de référentiel AWS CodeCommit par défaut ou entrez-en un différent. Passez ensuite à l'étape 9.
8. Si vous le souhaitez GitHub, vous devez choisir ou créer une ressource de connexion. Si vous avez déjà une connexion, sélectionnez-la dans le champ de recherche. Dans le cas contraire, créez une nouvelle connexion dès maintenant. Choisissez Connect to GitHub.

La page Créer une connexion s'affiche.

 Note

Pour créer une connexion, vous devez disposer d'un GitHub compte. Si vous créez une connexion pour une organisation, vous devez en être le propriétaire.



- a. Sous Créer une connexion à GitHub l'application, dans le champ de saisie du nom de la connexion, entrez le nom de votre connexion. Choisissez Connect to GitHub.

La GitHub page Connect to affiche et affiche le champ GitHub Applications.

- b. 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.

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

Note

Si vous avez déjà installé l'application, vous pouvez choisir Configurer (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.

- d. Si la page Confirmer le mot de passe pour continuer s'affiche, entrez votre GitHub mot de passe, puis choisissez Se connecter.
- e. Sur la GitHub page Installer le AWS connecteur pour, conservez les valeurs par défaut et choisissez Installer.


- f. Sur la GitHub page Connect to, l'identifiant d'installation de votre nouvelle installation apparaît dans le champ de saisie de texte GitHub Apps.


Une fois la connexion créée, sur la page de CodeStar création de projet, le message Ready to connect s'affiche.


Note

Vous pouvez consulter votre connexion dans les paramètres de la console Developer Tools. Pour plus d'informations, voir [Commencer à utiliser les connexions](#).

Select a repository provider


CodeCommit
Use a new AWS CodeCommit repository for your project. 

GitHub
Use a new GitHub source repository for your project (requires an existing GitHub account). 

 **The GitHub repository provider now uses CodeStar Connections**
To use a GitHub repository in CodeStar, create a connection. The connection will use GitHub Apps to access your repository. Use the following options to choose an existing connection or create a new one. [Learn more](#)

Connection
Choose an existing connection or create a new one and then return to this task.

or

 **Ready to connect**
Your Github connection is ready for use.


Repository owner
The owner of the new repository. This can be a personal GitHub account or a GitHub organization.

Repository name
The name of the new repository.

Repository description
An optional description of the new repository.


Public

- g. Pour Propriétaire du référentiel, choisissez l' GitHub organisation ou votre GitHub compte personnel.
- h. Pour Nom du référentiel, acceptez le nom du GitHub référentiel par défaut ou saisissez-en un autre.
- i. Choisissez Public ou Privé.

 Note


Pour l'utiliser AWS Cloud9 comme environnement de développement, vous devez sélectionner Public.

- j. (Facultatif) Dans Description du référentiel, entrez une description pour le GitHub référentiel.

 Note

Si vous choisissez un modèle de projet Alexa Skill, vous devez connecter un compte développeur Amazon. Pour plus d'informations sur l'utilisation des projets Alexa Skill, consultez [Tutoriel : créer un projet de compétence Alexa dans AWS CodeStar](#).

- 9. Si votre projet est déployé sur des instances Amazon EC2 et que vous souhaitez apporter des modifications, configurez vos instances Amazon EC2 dans Configuration Amazon EC2. Par exemple, vous pouvez choisir des types d'instances disponibles pour votre projet.

 Note

Les différents types d'instances Amazon EC2 fournissent différents niveaux de puissance de calcul et peuvent entraîner des coûts associés différents. Pour plus d'informations, consultez les [types d'instances Amazon EC2 et les tarifs Amazon EC2](#). Si vous avez plusieurs clouds privés virtuels (VPC) ou plusieurs sous-réseaux créés dans Amazon Virtual Private Cloud, vous pouvez également choisir le VPC et le sous-réseau à utiliser. Toutefois, si vous choisissez un type d'instance Amazon EC2 qui n'est pas pris en charge sur les instances dédiées, vous ne pouvez pas choisir un VPC dont la location d'instance est définie sur Dedicated. Pour plus d'informations, consultez [Qu'est-ce qu'Amazon VPC ?](#) et les [bases des instances dédiées](#).

Dans Key pair, choisissez la paire de clés Amazon EC2 que vous avez créée dans. [Étape 4 : Création d'une paire de clés Amazon EC2 pour les projets AWS CodeStar](#) Sélectionnez Je reconnais avoir accès au fichier de clé privée.

10. Choisissez Suivant.
11. Examinez les ressources et les détails de configuration.
12. Choisissez Suivant ou Créer un projet. (Le choix affiché dépend de votre modèle de projet.)

La création du projet, y compris du référentiel, peut prendre quelques minutes.

13. Une fois que votre projet dispose d'un référentiel, vous pouvez utiliser la page Référentiel pour configurer l'accès à celui-ci. Utilisez les liens des étapes suivantes pour configurer un IDE, configurer le suivi des problèmes ou ajouter des membres de l'équipe à votre projet.

Étape 2 : ajouter des informations d'affichage pour votre profil AWS CodeStar utilisateur

Lorsque vous créez un projet, vous êtes ajouté à l'équipe de projet comme propriétaire. Si c'est la première fois que vous utilisez AWS CodeStar, vous êtes invité à préciser les éléments suivants :

- Votre nom d'affichage à présenter aux autres utilisateurs.
- L'adresse e-mail à présenter aux autres utilisateurs.

Ces informations sont utilisées dans votre profil utilisateur AWS CodeStar. Les profils utilisateur ne sont pas spécifiques au projet, mais ils sont limités à une région AWS. Vous devez créer un profil utilisateur dans chaque AWS région dans laquelle vous appartenez à des projets. Chaque profil peut contenir des informations différentes si vous le souhaitez.

Saisissez un nom d'utilisateur et une adresse e-mail, puis cliquez sur Suivant.

Note

Ce nom d'utilisateur et cette adresse e-mail sont utilisés dans votre profil utilisateur AWS CodeStar. Si votre projet utilise des ressources extérieures AWS (par exemple, un GitHub référentiel ou des problèmes dans Atlassian JIRA), ces fournisseurs de ressources peuvent avoir leur propre profil utilisateur, avec des noms d'utilisateur et des adresses e-mail

différents. Pour plus d'informations, référez-vous à la documentation du fournisseur de la ressource.

Étape 3 : Afficher votre projet

La page de votre AWS CodeStar projet est l'endroit où vous et votre équipe pouvez consulter l'état des ressources de votre projet, y compris les dernières validations apportées à votre projet, l'état de votre pipeline de livraison continue et les performances de vos instances. Pour obtenir plus d'informations sur l'une de ces ressources, sélectionnez la page correspondante dans la barre de navigation.

Dans votre nouveau projet, la barre de navigation contient les pages suivantes :

- La page Vue d'ensemble contient des informations sur l'activité de votre projet, les ressources du projet et le README contenu de votre projet.
- La page IDE vous permet de connecter votre projet à un environnement de développement intégré (IDE) pour modifier, tester et appliquer les modifications du code source. Il contient des instructions pour configurer les IDE à la fois pour les AWS CodeCommit référentiels GitHub et des informations sur vos AWS Cloud9 environnements.
- La page Référentiel affiche les détails de votre dépôt, notamment le nom, le fournisseur, la date de sa dernière modification et les URL de clonage. Vous pouvez également consulter les informations relatives au dernier commit et consulter et créer des pull requests.
- La page Pipeline affiche les informations CI/CD relatives à votre pipeline. Vous pouvez consulter les détails du pipeline tels que le nom, l'action la plus récente et le statut. Vous pouvez consulter l'historique du pipeline et publier une modification. Vous pouvez également consulter le statut des différentes étapes de votre pipeline.
- La page de surveillance affiche Amazon EC2 ou des AWS Lambda métriques en fonction de la configuration de votre projet. Par exemple, il affiche l'utilisation du processeur de toutes les instances Amazon EC2 déployées AWS Elastic Beanstalk ou CodeDeploy des ressources de votre pipeline. Dans les projets qui utilisent AWS Lambda, il affiche les métriques d'appel et d'erreur pour la fonction Lambda. Ces informations s'affichent sur une base horaire. Si vous avez utilisé le modèle de AWS CodeStar projet suggéré pour ce didacticiel, vous devriez constater un pic d'activité notable lorsque votre application sera déployée pour la première fois sur ces instances. Vous pouvez actualiser la surveillance pour voir les modifications de l'état des instances, ce qui peut vous aider à identifier les problèmes ou la nécessité d'ajouter des ressources.

- La page Problèmes permet d'intégrer votre AWS CodeStar projet à un projet Atlassian JIRA. La configuration de cette vignette vous permet, ainsi que votre équipe de projet, de suivre les problèmes JIRA dans le tableau de bord du projet.

Le volet de navigation situé sur le côté gauche de la console vous permet de naviguer entre les pages Projet, Équipe et Paramètres.

Étape 4 : valider une modification

Tout d'abord, examinez l'exemple d'application inclus dans votre projet. Découvrez à quoi ressemble l'application en choisissant Afficher l'application depuis n'importe quel endroit de la navigation de votre projet. Votre exemple d'application Web sera affiché dans une nouvelle fenêtre ou dans un nouvel onglet de navigateur. C'est l'exemple de code de projet qu'AWS CodeStar a généré et déployé.

Si vous souhaitez consulter le code, dans la barre de navigation, sélectionnez Repository. Cliquez sur le lien sous Nom du référentiel et le référentiel de votre projet s'ouvre dans un nouvel onglet ou une nouvelle fenêtre. Lisez le contenu du fichier readme du référentiel (README.md) et parcourez le contenu des fichiers.

Au cours de cette étape, vous modifiez le code, puis vous publiez ce changement dans votre référentiel. Vous pouvez effectuer cette opération de plusieurs manières :

- Si le code du projet est stocké dans un GitHub référentiel CodeCommit OR, vous pouvez l'utiliser AWS Cloud9 pour travailler avec le code directement depuis votre navigateur Web, sans installer d'outils. Pour plus d'informations, veuillez consulter [Création d'un environnement AWS Cloud9 pour un projet](#).
- Si le code du projet est stocké dans un CodeCommit référentiel et que Visual Studio ou Eclipse sont installés, vous pouvez utiliser le AWS Toolkit for Visual Studio ou AWS Toolkit for Eclipse pour vous connecter plus facilement au code. Pour plus d'informations, veuillez consulter [Utilisation d'un IDE avec AWS CodeStar](#). Si vous ne possédez ni Visual Studio, ni Eclipse, installez un client Git et suivez les instructions figurant plus loin dans cette étape.
- Si le code du projet est stocké dans un GitHub référentiel, vous pouvez utiliser les outils de votre IDE pour vous y connecter GitHub.
 - Pour Visual Studio, vous pouvez utiliser des outils tels que l' GitHub extension pour Visual Studio. Pour plus d'informations, consultez la page de [présentation](#) sur le site Web de l' GitHub

extension pour Visual Studio et [Getting Started with GitHub for Visual Studio](#) sur le GitHub site Web.

- Pour Eclipse, vous pouvez utiliser un outil tel qu'EGit pour Eclipse. Pour plus d'informations, consultez la [documentation EGit](#) sur le site web EGit.
- Pour les autres IDE, consultez la documentation de l'IDE concerné.
- Pour les autres types de référentiels de code, consultez la documentation du fournisseur du référentiel.

Les instructions ci-dessous expliquent comment apporter une modification mineure à l'exemple.

Pour configurer votre ordinateur pour valider les modifications (utilisateur IAM)

Note

Dans cette procédure, nous supposons que le code de votre projet est stocké dans un référentiel CodeCommit. Pour les autres types de référentiels de code, reportez-vous à la documentation du fournisseur du référentiel, puis passez directement à la procédure suivante, [Pour cloner le référentiel de projet et effectuer une modification](#).

Si le code est stocké dans CodeCommit et que vous l'utilisez déjà CodeCommit ou si vous avez utilisé la AWS CodeStar console pour créer un environnement de AWS Cloud9 développement pour le projet, vous n'avez pas besoin de configuration supplémentaire. Passez à la procédure suivante, [Pour cloner le référentiel de projet et effectuer une modification](#).

1. [Installez Git](#) sur votre ordinateur local.
2. Connectez-vous à l'outil AWS Management Console, puis ouvrez la console IAM à l'adresse <https://console.aws.amazon.com/iam/>.

Connectez-vous en tant qu'utilisateur IAM qui utilisera les informations d'identification Git pour les connexions au référentiel de votre AWS CodeStar projet dans CodeCommit.

3. Dans la console IAM, dans le volet de navigation, choisissez Utilisateurs, puis dans la liste des utilisateurs, choisissez votre utilisateur IAM.
4. Sur la page des détails de l'utilisateur, choisissez l'onglet Security Credentials, puis dans HTTPS Git credentials for CodeCommit, sélectionnez Generate.

Note

Vous ne pouvez pas choisir vos propres identifiants de connexion pour les identifiants Git. Pour plus d'informations, consultez [Utiliser les informations d'identification Git et HTTPS avec CodeCommit](#).

5. Copiez les informations de connexion qu'IAM a générées pour vous. Vous pouvez choisir Afficher et copier-coller ces informations dans un fichier sécurisé sur votre ordinateur local, ou choisir Télécharger les informations d'identification pour télécharger ces informations sous la forme d'un fichier CSV. Vous avez besoin de ces informations pour vous connecter à CodeCommit.

Après avoir enregistré vos informations d'identification, choisissez Close.

Important

C'est votre seule chance de sauvegarder les informations de connexion. Si vous ne les enregistrez pas, vous pouvez copier le nom d'utilisateur depuis la console IAM, mais vous ne pouvez pas rechercher le mot de passe. Vous devrez alors réinitialiser le mot de passe puis l'enregistrer.

Pour configurer votre ordinateur pour valider les modifications (utilisateur fédéral)

Vous pouvez utiliser la console pour charger des fichiers dans votre référentiel, ou vous pouvez utiliser Git pour vous connecter à partir de votre ordinateur local. Si vous utilisez un accès fédéré, suivez cette procédure pour utiliser Git pour vous connecter et cloner un référentiel à partir de votre ordinateur local.

Note

Dans cette procédure, nous supposons que le code de votre projet est stocké dans un référentiel CodeCommit. Pour les autres types de référentiels de code, reportez-vous à la documentation du fournisseur du référentiel, puis passez directement à la procédure suivante, [Pour cloner le référentiel de projet et effectuer une modification](#).

1. [Installez Git](#) sur votre ordinateur local.

2. [Installez l'AWS CLI.](#)
3. Configurez vos informations d'identification de sécurité temporaires pour un utilisateur fédéré. Pour plus d'informations, consultez la section [Accès temporaire aux CodeCommit référentiels.](#) Les informations d'identification temporaires sont composées de :
 - Clé d'accès AWS
 - AWSclé secrète
 - Jeton de session

Pour plus d'informations sur les informations d'identification temporaires, consultez la section [Autorisations pour GetFederationToken.](#)

4. Connectez-vous à votre référentiel à l'aide de l'assistant d'informations d'identifications AWS CLI. Pour plus d'informations, voir [Étapes de configuration pour les connexions HTTPS CodeCommit aux référentiels sous Linux, macOS ou Unix avec l'assistant d'identification AWS CLI](#) ou [Étapes de configuration pour les connexions HTTPS aux CodeCommit référentiels sous Windows avec l'assistant d'identification CLI AWS](#)
5. L'exemple suivant montre comment se connecter à un CodeCommit dépôt et y envoyer un commit.

Exemple : Pour cloner le référentiel de projet et effectuer une modification

Note

Cette procédure explique comment cloner le référentiel de code du projet sur votre ordinateur, modifier le fichier `index.html` du projet, puis publier votre modification dans le référentiel distant. Dans cette procédure, nous partons du principe que le code de votre projet est stocké dans un CodeCommit dépôt et que vous utilisez un client Git depuis la ligne de commande. Pour les autres types de référentiels de code ou d'outils, reportez-vous à la documentation du fournisseur pour savoir comment cloner le référentiel, modifier le fichier, puis publier le code.

1. Si vous utilisez la console AWS CodeStar pour créer un environnement de développement AWS Cloud9 pour le projet, ouvrez l'environnement de développement, puis passez directement

à l'étape 3 de cette procédure. Pour ouvrir l'environnement de développement, consultez [Ouverture d'un environnement AWS Cloud9 pour un projet](#).

Votre projet étant ouvert dans la AWS CodeStar console, dans la barre de navigation, choisissez Repository. Dans Clone URL, choisissez le protocole pour le type de connexion que vous avez configuré CodeCommit, puis copiez le lien. Par exemple, si vous avez suivi les étapes de la procédure précédente pour configurer les informations d'identification Git pour CodeCommit, choisissez HTTPS.

2. Sur votre ordinateur local, ouvrez une fenêtre de terminal ou de ligne de commande et accédez au répertoire temporaire. Exécutez la commande `git clone` pour cloner le référentiel sur votre ordinateur. Collez le lien que vous avez copié. Par exemple, pour CodeCommit utiliser le protocole HTTPS :

```
git clone https://git-codecommit.us-east-2.amazonaws.com/v1/repos/my-first-projec
```

La première fois que vous vous connectez, vous êtes invité à saisir les informations d'identification du référentiel. Pour CodeCommit, entrez les informations d'identification Git que vous avez téléchargées lors de la procédure précédente.

3. Accédez au répertoire cloné sur votre ordinateur et parcourez son contenu.
4. Ouvrez le fichier `index.html` (dans le dossier public) et apportez une modification au fichier. Par exemple, ajoutez un paragraphe après la balise `<H2>`, tel que :

```
<P>Hello, world!</P>
```

Sauvegardez le fichier.

5. Depuis un terminal ou une invite de commande, ajoutez votre fichier modifié, puis validez et transmettez votre modification en mode push :

```
git add index.html
git commit -m "Making my first change to the web app"
git push
```

6. Sur la page Référentiel, consultez les modifications en cours. Vous devriez voir que l'historique des validations de votre référentiel est mis à jour avec votre validation et vous apercevez aussi le message de validation. Sur la page Pipeline, vous pouvez voir le pipeline récupérer vos modifications apportées au référentiel et commencer à le créer et à le déployer. Une fois

votre application Web déployée, vous pouvez choisir Afficher l'application pour afficher votre modification.

Note

Si la mention Échoué est affichée pour l'une des étapes du pipeline, consultez les ressources de dépannage suivantes :

- Pour l'étape Source, voir [Résolution des problèmes AWS CodeCommit](#) dans le Guide de AWS CodeCommit l'utilisateur.
- Pour la phase de génération, consultez la section [Résolution des problèmes AWS CodeBuild](#) dans le guide de AWS CodeBuild l'utilisateur.
- Pour la phase de déploiement, consultez la section [Résolution des problèmes AWS CloudFormation](#) dans le guide de AWS CloudFormation l'utilisateur.
- Pour les autres problèmes, consultez [Résolution des problèmes AWS CodeStar](#).

Étape 5 : Ajouter d'autres membres à l'équipe

Chaque projet AWS CodeStar est déjà configuré avec trois rôles AWS CodeStar. Chaque rôle fournit son propre niveau d'accès au projet et à ses ressources :

- Propriétaire : peut ajouter et supprimer des membres de l'équipe, modifier le tableau de bord du projet et supprimer le projet.
- Contributeur : peut modifier le tableau de bord du projet et contribuer au code si le code y est stocké CodeCommit, mais il est impossible d'ajouter ou de supprimer des membres de l'équipe ou de supprimer le projet. C'est le rôle que vous devez choisir pour la plupart des membres de l'équipe dans un projet AWS CodeStar.
- Afficheur : peut afficher le tableau de bord du projet, le code du projet s'il est stocké et l'état du projet, mais il ne peut pas déplacer, ajouter ou supprimer des vignettes du tableau de bord du projet. CodeCommit

⚠ Important

Si votre projet utilise des ressources extérieures AWS (par exemple, un GitHub référentiel ou des problèmes dans Atlassian JIRA), l'accès à ces ressources est contrôlé par le fournisseur de ressources, et non. AWS CodeStar Pour plus d'informations, référez-vous à la documentation du fournisseur de la ressource.

Toute personne ayant accès à un projet AWS CodeStar peut être en mesure d'utiliser la console AWS CodeStar pour accéder à des ressources qui sont en dehors d'AWS, mais qui sont associées au projet.

AWS CodeStar n'autorise pas les membres de l'équipe de projet à participer à un environnements de développement AWS Cloud9 associé pour un projet. Pour autoriser un membre de l'équipe à participer à un environnement partagé, consultez [Partage d'un environnement AWS Cloud9 avec un membre de l'équipe de projet](#).

Pour plus d'informations sur les équipes et les rôles de projet, consultez [Utilisation des équipes AWS CodeStar](#).

Pour ajouter un membre de l'équipe à un projet AWS CodeStar (console)


1. Ouvrez la AWS CodeStar console à l'[adresse https://console.aws.amazon.com/codestar/](https://console.aws.amazon.com/codestar/).
2. Choisissez Projets dans le volet de navigation et choisissez votre projet.
3. Dans le volet de navigation latéral du projet, choisissez Team.
4. Sur la page Team members (Membres d'équipe), choisissez Ajouter un membre d'équipe.
5. Dans Choose user (Choisir un utilisateur), effectuez l'une des actions suivantes :
 - Si un utilisateur IAM existe déjà pour la personne que vous souhaitez ajouter, choisissez-le dans la liste.

i Note

Les utilisateurs qui ont déjà été ajoutés à un autre AWS CodeStar projet apparaissent dans la liste des AWS CodeStarutilisateurs existants.

Dans Rôle du projet, choisissez le AWS CodeStar rôle (propriétaire, contributeur ou spectateur) de cet utilisateur. C'est un rôle de niveau projet AWS CodeStar qui ne peut être


modifié que par un propriétaire du projet. Lorsqu'il est appliqué à un utilisateur IAM, le rôle fournit toutes les autorisations requises pour accéder aux ressources AWS CodeStar du projet. Il applique les politiques requises pour créer et gérer les informations d'identification Git pour le code stocké CodeCommit dans IAM ou pour télécharger les clés SSH Amazon EC2 pour l'utilisateur dans IAM.

 Important

Vous ne pouvez pas fournir ou modifier le nom d'affichage ou les informations de courrier électronique d'un utilisateur IAM à moins d'être connecté à la console en tant qu'utilisateur. Pour plus d'informations, veuillez consulter [Gérer les informations d'affichage pour votre profil utilisateur AWS CodeStar](#).

Choisissez Ajouter un membre de l'équipe.

- Si aucun utilisateur IAM n'existe pour la personne que vous souhaitez ajouter au projet, choisissez Create new IAM user. Vous serez redirigé vers la console IAM où vous pourrez créer un nouvel utilisateur IAM. Pour plus d'informations, reportez-vous à la section [Création d'utilisateurs IAM](#) dans le guide de l'utilisateur IAM. Après avoir créé votre utilisateur IAM, revenez à la AWS CodeStar console, actualisez la liste des utilisateurs et choisissez l'utilisateur IAM que vous avez créé dans la liste déroulante. Entrez le nom AWS CodeStar d'affichage, l'adresse e-mail et le rôle de projet que vous souhaitez appliquer à ce nouvel utilisateur, puis choisissez Ajouter un membre de l'équipe.

 Note

Pour faciliter la gestion, le rôle Propriétaire doit être attribué à au moins un utilisateur du projet.

6. Envoyez les informations suivantes au nouveau membre de l'équipe :

- Informations de connexion pour votre projet AWS CodeStar.
- Si le code source est stocké dans CodeCommit des [instructions pour configurer l'accès au CodeCommit référentiel à l'aide des informations d'identification Git](#) à partir de leurs ordinateurs locaux.

- Informations sur la façon dont l'utilisateur peut gérer son nom d'affichage, son adresse e-mail et sa clé SSH publique Amazon EC2, comme décrit dans. [Utilisation de votre profil utilisateur AWS CodeStar](#)
- Mot de passe et informations de connexion à usage unique, si l'utilisateur est nouveau AWS et que vous avez créé un utilisateur IAM pour cette personne. Le mot de passe expire à la première connexion de l'utilisateur. L'utilisateur doit choisir un nouveau mot de passe.

Étape 6 : Nettoyage

Félicitations ! Vous avez terminé le didacticiel. Si vous ne voulez pas continuer à utiliser ce projet et ses ressources, vous devez le supprimer de façon à éviter la facturation d'éventuels frais continus sur votre compte AWS.

Pour supprimer un projet dans AWS CodeStar

1. Ouvrez la AWS CodeStar console à l'[adresse https://console.aws.amazon.com/codestar/](https://console.aws.amazon.com/codestar/).
2. Choisissez Projets dans le volet de navigation.
3. Sélectionnez le projet que vous souhaitez supprimer, puis cliquez sur Supprimer.

Vous pouvez également ouvrir le projet et choisir Paramètres dans le volet de navigation situé sur le côté gauche de la console. Sur la page des détails du projet, choisissez Supprimer le projet.

4. Sur la page de confirmation de suppression, saisissez Supprimer. Maintenez l'option Supprimer les ressources sélectionnée si vous souhaitez supprimer les ressources du projet. Choisissez Delete (Supprimer).

Le processus de suppression d'un projet peut prendre plusieurs minutes. Une fois que le projet est supprimé, il ne s'affiche plus dans la liste des projets dans la console AWS CodeStar.

Important

Si votre projet utilise des ressources extérieures AWS (par exemple, un GitHub référentiel ou des problèmes dans Atlassian JIRA), ces ressources ne sont pas supprimées, même si vous cochez la case.

Votre projet ne peut pas être supprimé si des stratégies gérées AWS CodeStar ont été attachées manuellement à des rôles qui ne correspondent pas à des utilisateurs IAM. Si vous avez attaché l'une des stratégies gérées de votre projet au rôle d'un

utilisateur fédéré, vous devez la détacher avant de pouvoir supprimer le projet. Pour plus d'informations, veuillez consulter [???](#).

Étape 7 : Préparez votre projet pour un environnement de production

Une fois que vous avez créé votre projet, vous êtes prêt à créer, tester et déployer le code. Tenez compte des points suivants pour gérer votre projet dans un environnement de production :

- Appliquez régulièrement des correctifs et consultez les bonnes pratiques en matière de sécurité pour les dépendances utilisées par votre application. Pour plus d'informations, veuillez consulter [Bonnes pratiques de sécurité pour les ressources AWS CodeStar](#).
- Surveillez régulièrement les paramètres d'environnement proposés par le langage de programmation de votre projet.

Étapes suivantes

Voici d'autres ressources pour vous aider à en savoir plus sur AWS CodeStar :

- Il [Didacticiel : Création et gestion d'un projet sans serveur dans AWS CodeStar](#) utilise un projet qui crée et déploie un service Web à l'aide de la logique AWS Lambda et qui peut être appelé par une API dans Amazon API Gateway.
- [Modèles de projet AWS CodeStar](#) décrit d'autres types de projets que vous pouvez créer.
- [Utilisation des équipes AWS CodeStar](#) offre des informations sur l'activation d'autres utilisateurs qui collaboreront avec vous sur vos projets.

Didacticiel : Création et gestion d'un projet sans serveur dans AWS CodeStar

Dans ce didacticiel, vous allez utiliser AWS CodeStar pour créer un projet qui utilise le modèle d'application sans serveur AWS (AWS SAM) afin de créer et gérer des ressources AWS pour un service web hébergé dans AWS Lambda.

AWS CodeStar utilise AWS SAM, qui s'appuie sur AWS CloudFormation, pour simplifier la création et la gestion des AWS ressources prises en charge, notamment les API, les AWS Lambda fonctions et les tables Amazon DynamoDB d'Amazon API Gateway. (Ce projet n'utilise aucune table Amazon DynamoDB.)

Pour plus d'informations, consultez la section [Modèle d'application AWS sans serveur \(AWSSAM\)](#) sur GitHub.

Prérequis : Effectuez les étapes détaillées dans [Configuration AWS CodeStar](#).

Note

Des coûts liés à ce didacticiel peuvent être facturés sur votre compte AWS, dont des frais pour les services AWS utilisés par AWS CodeStar. Pour plus d'informations, consultez [AWS CodeStar Pricing](#) (Tarification CTlong).

Rubriques

- [Présentation](#)
- [Étape 1 : création du projet](#)
- [Étape 2 : Parcourir les ressources du projet](#)
- [Étape 3 : Tester le service web](#)
- [Étape 4 : Configurer votre poste de travail local pour modifier le code du projet](#)
- [Étape 5 : Ajouter la logique au service web](#)
- [Étape 6 : Tester le service web amélioré](#)
- [Étape 7 : Ajouter un test unitaire pour le service web](#)
- [Étape 8 : Afficher les résultats du test unitaire](#)
- [Étape 9 : Nettoyer](#)
- [Étapes suivantes](#)

Présentation

Dans ce tutoriel :

1. Vous utilisez AWS CodeStar pour créer un projet qui utilise AWS SAM afin de générer et déployer un service web basé sur Python. Ce service Web est hébergé dans Amazon API Gateway AWS Lambda et est accessible via Amazon API Gateway.
2. Vous parcourez les ressources principales du projet, qui incluent :
 - Le référentiel AWS CodeCommit où le code source du projet est stocké. Ce code source inclut la logique du service web et définit les ressources AWS connexes.
 - Le pipeline AWS CodePipeline qui automatise la génération du code source. Ce pipeline utilise AWS SAM pour créer et déployer une fonction AWS Lambda, créer une API associée dans Amazon API Gateway et connecter l'API à la fonction.
 - La fonction qui est déployée sur AWS Lambda.
 - L'API créée dans Amazon API Gateway.
3. Vous testez le service web pour vérifier qu'AWS CodeStar a généré et déployé le service web comme prévu.
4. Vous configurez votre poste de travail local afin qu'il fonctionne avec le code source du projet.
5. Vous modifiez le code source du projet à l'aide de votre poste de travail local. Lorsque vous ajoutez une fonction au projet, puis transmettez vos modifications au code source, AWS CodeStar recrée et redéploie le service web.
6. Vous testez à nouveau le service web pour vérifier qu'AWS CodeStar a recréé et redéployé le service web comme prévu.
7. Vous écrivez un test unitaire à l'aide de votre poste de travail local pour remplacer certains de vos tests manuels par un test automatisé. Lorsque vous transmettez le test unitaire, AWS CodeStar recrée et redéploie le service web, puis exécute le test unitaire.
8. Vous affichez les résultats des tests unitaires.
9. Vous nettoyez le projet. Cette étape permet d'éviter que ne soient facturés sur votre compte AWS les coûts liés à ce didacticiel.

Étape 1 : création du projet

Au cours de cette étape, vous utilisez la console AWS CodeStar pour créer un projet.

1. Connectez-vous à la AWS CodeStar console AWS Management Console et ouvrez-la à l'adresse <https://console.aws.amazon.com/codestar/>.

Note

Vous devez vous connecter à l'AWS Management Console aide des informations d'identification associées à l'utilisateur IAM que vous avez créé ou dans [Configuration AWS CodeStar](#) lequel vous vous êtes identifié. Cet utilisateur doit disposer de la stratégie gérée **AWSCodeStarFullAccess** attachée.

2. Choisissez la région AWS dans laquelle vous souhaitez créer le projet et ses ressources.

Pour plus d'informations sur les régions AWS dans lesquelles AWS CodeStar est disponible, consultez [Régions et points de terminaison](#) dans le document Référence générale AWS.

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

4. Sur la page Choisir un modèle de projet :

- Pour Type d'application, sélectionnez Service Web.
- Dans Langage de programmation, sélectionnez Python.
- Pour le AWSservice, sélectionnez AWS Lambda.

5. Choisissez la case qui contient vos sélections. Choisissez Suivant.

6. Pour Nom du projet, entrez un nom pour le projet (par exemple, **My SAM Project**). Si vous utilisez un nom différent de celui de l'exemple, veillez à l'utiliser tout au long de ce didacticiel.

Pour ID de projet, AWS CodeStar choisit un identifiant associé pour ce projet (par exemple, my-sam-project). Si un ID de projet différent vous est proposé, veillez à l'utiliser tout au long de ce didacticiel.

Laissez AWS CodeCommit sélectionné et ne modifiez pas la valeur Nom du référentiel.

7. Choisissez Suivant.

8. Vérifiez vos paramètres, puis choisissez Créer un projet.

Si c'est la première fois que vous l'utilisez AWS CodeStar dans cette AWS région, dans Nom d'affichage et e-mail, entrez le nom d'affichage et l'adresse e-mail que vous AWS CodeStar souhaitez utiliser pour votre utilisateur IAM. Choisissez Suivant.

9. Attendez qu'AWS CodeStar crée le projet. Cela peut prendre plusieurs minutes. Ne poursuivez pas tant que la bannière provisionnée du projet ne s'affiche pas lorsque vous actualisez.

Étape 2 : Parcourir les ressources du projet

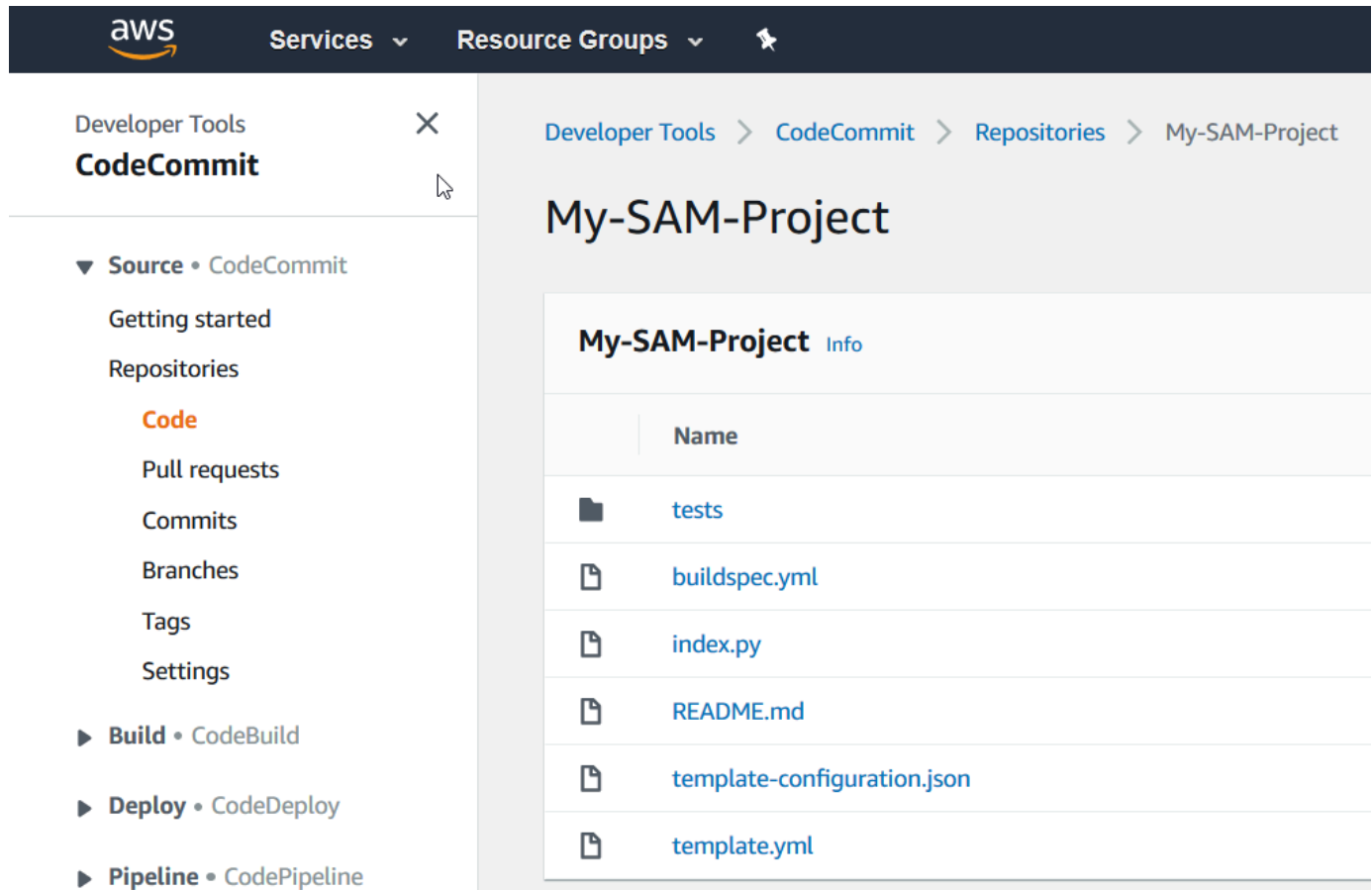
Au cours de cette étape, vous parcourez quatre des ressources AWS du projet pour comprendre la façon dont celui-ci fonctionne.

- Le AWS CodeCommit référentiel dans lequel le code source du projet est stocké. AWS CodeStar donne le nom au dépôt `my-sam-project`, où `my-sam-project` est le nom du projet.
- Le AWS CodePipeline pipeline qui utilise CodeBuild AWS SAM pour automatiser la création et le déploiement de la fonction Lambda et de l'API du service Web dans API Gateway. AWS CodeStar donne au pipeline le nom `my-sam-project--Pipeline`, où `my-sam-project` est l'ID du projet.
- Fonction Lambda qui contient la logique du service Web. AWS CodeStar donne à la fonction le nom `awscodestar-my-sam-project-lambda- HelloWorld - RANDOM_ID`, où :
 - `my-sam-project` est l'ID du projet.
 - `HelloWorld` est l'ID de fonction tel que spécifié dans le `template.yaml` fichier du AWS CodeCommit référentiel. Vous parcourrez ce fichier ultérieurement.
 - ***ID_ALÉATOIRE*** est un ID aléatoire attribué par AWS SAM à la fonction pour garantir son caractère unique.
- L'API d'API Gateway qui facilite l'appel de la fonction Lambda. AWS CodeStar donne à l'API le nom `awscodestar-my-sam-project--lambda`, où `my-sam-project` est l'ID du projet.

Pour explorer le référentiel de code source dans CodeCommit

1. Votre projet étant ouvert dans la AWS CodeStar console, dans la barre de navigation, choisissez Repository.
2. Choisissez le lien vers votre CodeCommit dépôt (**My-SAM-Project**) dans Détails du dépôt.
3. Dans la CodeCommit console, sur la page Code, les fichiers de code source du projet sont affichés :
 - `buildspec.yaml`, qui CodePipeline indique CodeBuild à utiliser pendant la phase de construction pour emballer le service Web à l'aide de AWS SAM.
 - `index.py`, qui contient la logique de la fonction Lambda. Cette fonction génère simplement la chaîne `Hello World`, ainsi qu'un horodatage au format ISO.
 - `README.md`, qui contient des informations générales sur le référentiel.
 - `template-configuration.json`, qui contient l'ARN du projet avec des espaces réservés utilisés pour marquer les ressources avec l'ID du projet

- `template.yml`, que AWS SAM utilise pour emballer le service Web et créer l'API dans API Gateway.



Pour afficher le contenu d'un fichier, sélectionnez ce dernier dans la liste.

Pour plus d'informations sur l'utilisation de la CodeCommit console, consultez le [guide de AWS CodeCommit l'utilisateur](#).

Pour explorer le pipeline dans CodePipeline

1. Pour afficher des informations sur le pipeline, avec votre projet ouvert dans la AWS CodeStar console, dans la barre de navigation, choisissez Pipeline et vous verrez que le pipeline contient :
 - Une phase Source pour obtenir le code source à partir d' CodeCommit.
 - Une phase Création pour générer le code source avec CodeBuild.

- Une phase Déploiement pour déployer le code source généré et les ressources AWS avec AWS SAM.
2. Pour afficher plus d'informations sur le pipeline, dans Détails du pipeline, choisissez votre pipeline pour l'ouvrir dans la CodePipeline console.

Pour plus d'informations sur l'utilisation de la CodePipeline console, consultez le [guide de AWS CodePipeline l'utilisateur](#).

Pour explorer les activités du projet et les ressources AWS de service sur la page de présentation

1. Ouvrez votre projet dans la AWS CodeStar console et dans la barre de navigation, sélectionnez Vue d'ensemble.
2. Consultez les listes des activités du projet et des ressources du projet.

Pour explorer la fonction dans Lambda

1. Votre projet étant ouvert dans la AWS CodeStar console, dans la barre de navigation latérale, choisissez Vue d'ensemble.
2. Dans Ressources du projet, dans la colonne ARN, choisissez le lien pour la fonction Lambda.

Le code de la fonction est affiché dans la console Lambda.

Pour plus d'informations sur l'utilisation de la console Lambda, consultez le manuel du [AWS Lambda développeur](#).

Pour explorer l'API dans API Gateway

1. Votre projet étant ouvert dans la AWS CodeStar console, dans la barre de navigation latérale, choisissez Vue d'ensemble.
2. Dans Ressources du projet, dans la colonne ARN, choisissez le lien vers l'API Amazon API Gateway.

Les ressources de l'API sont affichées dans la console API Gateway.

Pour plus d'informations sur l'utilisation de la console API Gateway, consultez le [guide du développeur d'API Gateway](#).

Étape 3 : Tester le service web

Au cours de cette étape, vous testez le service web qu'AWS CodeStar vient de générer et de déployer.

1. Votre projet étant toujours ouvert par rapport à l'étape précédente, dans la barre de navigation, choisissez Pipeline.
2. Assurez-vous que le message Succeeded est affiché pour les étapes Source, Build et Deploy avant de continuer. Cela peut prendre plusieurs minutes.

Note

Si la mention Échec est affichée pour l'une des phases, consultez les ressources de dépannage suivantes :

- Pour l'étape Source, voir [Résolution des problèmes AWS CodeCommit](#) dans le Guide de AWS CodeCommit l'utilisateur.
- Pour la phase de génération, consultez la section [Résolution des problèmes AWS CodeBuild](#) dans le guide de AWS CodeBuild l'utilisateur.
- Pour la phase de déploiement, consultez la section [Résolution des problèmes AWS CloudFormation](#) dans le guide de AWS CloudFormation l'utilisateur.
- Pour les autres problèmes, consultez [Résolution des problèmes AWS CodeStar](#).

3. Choisissez Afficher l'application.

Dans le nouvel onglet qui s'ouvre dans votre navigateur web, le service web affiche la sortie de réponse suivante :

```
{"output": "Hello World", "timestamp": "2017-08-30T15:53:42.682839"}
```


Étape 4 : Configurer votre poste de travail local pour modifier le code du projet

Dans cette étape, vous configurez votre poste de travail local pour modifier le code source dans le projet AWS CodeStar. Votre poste de travail local peut être un ordinateur physique ou virtuel exécutant macOS, Windows ou Linux.

1. Votre projet étant toujours ouvert depuis l'étape précédente :
 - Dans la barre de navigation, choisissez IDE, puis développez Accédez au code de votre projet.
 - Choisissez Afficher les instructions sous Interface de ligne de commande.

Si Visual Studio ou Eclipse est installé, choisissez plutôt Afficher les instructions sous Visual Studio ou Eclipse, suivez les instructions, puis passez à [Étape 5 : Ajouter la logique au service web](#).
2. Suivez les instructions pour réaliser les tâches suivantes :
 - a. Configurez Git sur votre poste de travail local.
 - b. Utilisez la console IAM pour générer des informations d'identification Git pour votre utilisateur IAM.
 - c. Clonez le CodeCommit dépôt du projet sur votre poste de travail local.
3. Dans le menu de navigation de gauche, choisissez Projet pour revenir à l'aperçu de votre projet.

Étape 5 : Ajouter la logique au service web

Au cours de cette étape, vous utilisez votre poste de travail local pour ajouter la logique au service web. Plus précisément, vous ajoutez une fonction Lambda, puis vous la connectez à l'API dans API Gateway.

1. Sur votre poste de travail local, accédez au répertoire qui contient le référentiel de code source cloné.
2. Dans ce répertoire, créez un fichier nommé `hello.py`. Ajoutez le code suivant, puis enregistrez le fichier :

```
import json

def handler(event, context):
```

```
data = {
  'output': 'Hello ' + event["pathParameters"]["name"]
}
return {
  'statusCode': 200,
  'body': json.dumps(data),
  'headers': {'Content-Type': 'application/json'}
}
```

Le code précédent génère la chaîne Hello en sortie, ainsi que la chaîne envoyée par l'auteur de l'appel à la fonction.

3. Dans le même répertoire, ouvrez le fichier `template.yml`. Ajoutez le code suivant à la fin du fichier, puis enregistrez ce dernier :


```
Hello:
  Type: AWS::Serverless::Function
  Properties:
    FunctionName: !Sub 'awscodestar-${ProjectId}-lambda-Hello'
    Handler: hello.handler
    Runtime: python3.7
    Role:
      Fn::GetAtt:
        - LambdaExecutionRole
        - Arn
    Events:
      GetEvent:
        Type: Api
        Properties:
          Path: /hello/{name}
          Method: get
```

AWSSAM utilise ce code pour créer une fonction dans Lambda, ajouter une nouvelle méthode et un nouveau chemin vers l'API dans API Gateway, puis connecter cette méthode et ce chemin à la nouvelle fonction.

Note


Il est très important de mettre en retrait le code qui précède. Si vous n'ajoutez pas le code exactement tel qu'il est affiché, le projet risque de ne pas être généré correctement.

4. Exécutez `git add .` pour ajouter les modifications apportées au fichier dans la zone de transit du référentiel cloné. N'oubliez pas le point (`.`), qui ajoute tous les fichiers modifiés.

 Note

Si vous utilisez Visual Studio ou Eclipse au lieu de la ligne de commande, les instructions pour l'utilisation de Git peuvent être différentes. Consultez la documentation de Visual Studio ou d'Eclipse.

5. Exécutez `git commit -m "Added hello.py and updated template.yaml."` pour valider vos fichiers intermédiaires dans le référentiel cloné
6. Exécutez `git push` pour publier votre validation dans le référentiel distant.

 Note

Il se peut que vous soyez invité à saisir les informations de connexion générées précédemment. Pour éviter d'être invité à réaliser cette opération chaque fois que vous interagissez avec le référentiel distant, vous pouvez installer et configurer un gestionnaire d'informations d'identification Git. Par exemple, sous macOS ou Linux, vous pouvez exécuter `git config credential.helper 'cache --timeout 900'` dans le terminal pour laisser un intervalle d'au moins 15 minutes entre chaque invite. Vous pouvez aussi exécuter `git config credential.helper 'store --file ~/.git-credentials'` pour ne plus jamais voir d'invitation. Git stocke vos informations d'identification en texte clair dans un fichier brut de votre répertoire de base. Pour plus d'informations, consultez [Git Tools - Credential Storage](#) sur le site web de Git.

Une fois le push AWS CodeStar détecté, il demande CodePipeline à AWS SAM de reconstruire CodeBuild et de redéployer le service Web. Vous pouvez suivre la progression du déploiement sur la page Pipeline.

*AWSSAM donne à la nouvelle fonction le nom **awscodestar-my-sam-project-Lambda-Hello-`RANDOM_ID`**, où :*

- `my-sam-project` est l'ID du projet.
- `Hello` est l'ID de fonction, tel que spécifié dans le fichier `template.yaml`.

- **ID_ALÉATOIRE** est un ID aléatoire attribué par AWS SAM à la fonction pour garantir son caractère unique.

Étape 6 : Tester le service web amélioré

Au cours de cette étape, vous avez l'occasion de tester le service web amélioré qu'AWS CodeStar a généré et déployé, à partir de la logique que vous avez ajoutée lors de l'étape précédente.

1. Votre projet étant toujours ouvert dans la AWS CodeStar console, dans la barre de navigation, choisissez Pipeline.
2. Assurez-vous que le pipeline a été réexécuté et que le message Succeeded est affiché pour les étapes Source, Build et Deploy avant de continuer. Cela peut prendre plusieurs minutes.

Note

Si la mention Échec est affichée pour l'une des phases, consultez les ressources de dépannage suivantes :

- Pour l'étape Source, voir [Résolution des problèmes AWS CodeCommit](#) dans le Guide de AWS CodeCommit l'utilisateur.
- Pour la phase de génération, consultez la section [Résolution des problèmes AWS CodeBuild](#) dans le guide de AWS CodeBuild l'utilisateur.
- Pour la phase de déploiement, consultez la section [Résolution des problèmes AWS CloudFormation](#) dans le guide de AWS CloudFormation l'utilisateur.
- Pour les autres problèmes, consultez [Résolution des problèmes AWS CodeStar](#).

3. Choisissez Afficher l'application.

Dans le nouvel onglet qui s'ouvre dans votre navigateur web, le service web affiche la sortie de réponse suivante :

```
{"output": "Hello World", "timestamp": "2017-08-30T15:53:42.682839"}
```

4. Dans la zone d'adresse de l'onglet, ajoutez le chemin d'accès **/hello/** et votre prénom à la fin de l'URL, (par exemple, `https://ID_API.execute-api.ID_RÉGION.amazonaws.com/Prod/hello/VOTRE_PRÉNOM`), puis appuyez sur Entrée.

Si votre prénom est Mary, le service web affiche la sortie de réponse suivante :

```
{"output": "Hello Mary"}
```

Étape 7 : Ajouter un test unitaire pour le service web

Au cours de cette étape, vous utilisez votre poste de travail local pour ajouter un test qu'AWS CodeStar exécute sur le service web. Ce test remplace les tests manuels que vous avez effectués précédemment.

1. Sur votre poste de travail local, accédez au répertoire qui contient le référentiel de code source cloné.
2. Dans ce répertoire, créez un fichier nommé `hello_test.py`. Ajoutez le code suivant, puis enregistrez le fichier.

```
from hello import handler

def test_hello_handler():

    event = {
        'pathParameters': {
            'name': 'testname'
        }
    }

    context = {}

    expected = {
        'body': '{"output": "Hello testname"}',
        'headers': {
            'Content-Type': 'application/json'
        },
        'statusCode': 200
    }

    assert handler(event, context) == expected
```

Ce test vérifie si la sortie de la fonction Lambda est au format attendu. Si tel est le cas, le test est réussi. Dans le cas contraire, le test échoue.

3. Dans le même répertoire, ouvrez le fichier `buildspec.yml`. Remplacez le contenu du fichier par le code suivant, puis enregistrez le fichier.

```
version: 0.2

phases:
  install:
    runtime-versions:
      python: 3.7

    commands:
      - pip install pytest
      # Upgrade AWS CLI to the latest version
      - pip install --upgrade awscli

  pre_build:
    commands:
      - pytest

  build:
    commands:
      # Use AWS SAM to package the application by using AWS CloudFormation
      - aws cloudformation package --template template.yml --s3-bucket
      $S3_BUCKET --output-template template-export.yml

      # Do not remove this statement. This command is required for AWS CodeStar
      projects.
      # Update the AWS Partition, AWS Region, account ID and project ID in the
      project ARN on template-configuration.json file so AWS CloudFormation can tag
      project resources.
      - sed -i.bak 's/\${PARTITION}\$/'${PARTITION}'/g;s/\${AWS_REGION}
      \$/'${AWS_REGION}'/g;s/\${ACCOUNT_ID}\$/'${ACCOUNT_ID}'/g;s/\${PROJECT_ID}\
      \$/'${PROJECT_ID}'/g' template-configuration.json

artifacts:
  type: zip
  files:
    - template-export.yml
```

```
- template-configuration.json
```

Cette spécification de construction indique d' CodeBuild installer pytest, le framework de test Python, dans son environnement de construction. CodeBuild utilise pytest pour exécuter le test unitaire. Le reste de la spécification de génération reste identique.

4. Utilisez Git pour transmettre ces modifications au référentiel distant.

```
git add .  
  
git commit -m "Added hello_test.py and updated buildspec.yml."  
  
git push
```

Étape 8 : Afficher les résultats du test unitaire

Au cours de cette étape, vous pouvez voir si le test unitaire a réussi ou échoué.

1. Votre projet étant toujours ouvert dans la AWS CodeStar console, dans la barre de navigation, choisissez Pipeline.
2. Assurez-vous que le pipeline a été réexécuté avant de continuer. Cela peut prendre plusieurs minutes.

Si le test unitaire a réussi, la mention Réussi s'affiche pour la phase Création.

3. Pour afficher les détails des résultats du test unitaire, dans la phase de construction, cliquez CodeBuild sur le lien.
4. Dans la CodeBuild console, sur la my-sam-project page Build Project :, dans l'historique des builds, cliquez sur le lien dans la colonne Build run du tableau.
5. Sur la page my-sam-project: **BUILD_ID**, dans Build logs, cliquez sur le lien Afficher l'intégralité du log.
6. Dans la console Amazon CloudWatch Logs, recherchez dans la sortie du journal un résultat de test similaire au suivant. Pour les résultats suivants, le test a été réussi :

```
...  
===== test session starts =====  
platform linux2 -- Python 2.7.12, pytest-3.2.1, py-1.4.34, pluggy-0.4.0  
rootdir: /codebuild/output/src123456789/src, inifile:  
collected 1 item
```

```
hello_test.py .  
  
===== 1 passed in 0.01 seconds =====  
...
```

Si le test a échoué, il devrait y avoir des détails dans la sortie de journal afin de vous aider à résoudre le problème.

Étape 9 : Nettoyer

Au cours de cette étape, vous nettoyez le projet afin d'éviter des frais permanents liés à ce projet.

Si vous souhaitez continuer à utiliser ce projet, vous pouvez ignorer cette étape, mais votre compte AWS risque d'être encore facturé.

1. Votre projet étant toujours ouvert dans la AWS CodeStar console, dans la barre de navigation, sélectionnez Paramètres.
2. Dans Détails du projet, choisissez Supprimer le projet.
3. Entrez **delete**, maintenez la case Supprimer les ressources sélectionnée, puis choisissez Supprimer.

Important

Si vous désactivez cette case, l'enregistrement du projet est supprimé d'AWS CodeStar, mais la plupart des ressources AWS du projet sont conservées. Votre compte AWS risque de continuer à être facturé.

Si un compartiment Amazon S3 a toujours AWS CodeStar été créé pour ce projet, procédez comme suit pour le supprimer. :

1. Ouvrez la console Amazon S3 à l'adresse <https://console.aws.amazon.com/s3/>.
2. *Dans la liste des buckets, choisissez l'icône à côté de **aws-codestar-REGION_ID - ACCOUNT_ID - --pipe**, où :*
 - **ID_RÉGION** est l'ID de la région AWS du projet que vous venez de supprimer.
 - **ID_COMPTE** est votre ID de compte AWS.

- my-sam-projectest l'ID du projet que vous venez de supprimer.
3. Choisissez Vider le compartiment. Entrez le nom du compartiment, puis choisissez Confirmer.
 4. Choisissez Supprimer le compartiment. Entrez le nom du compartiment, puis choisissez Confirmer.

Étapes suivantes

Maintenant que vous avez terminé ce didacticiel, nous vous suggérons de consulter les ressources suivantes :

- Le [Démarrer avec AWS CodeStar](#) didacticiel utilise un projet qui crée et déploie une application Web basée sur Node.js exécutée sur une instance Amazon EC2.
- [Modèles de projet AWS CodeStar](#) décrit d'autres types de projets que vous pouvez créer.
- [Utilisation des équipes AWS CodeStar](#) explique comment d'autres personnes peuvent vous aider sur vos projets.

Didacticiel : Création d'un projet dans AWS CodeStar à l'aide de l'AWS CLI

Ce didacticiel explique comment utiliser le pour AWS CLI créer un AWS CodeStar projet avec un exemple de code source et un exemple de modèle de chaîne d'outils. AWS CodeStarfournit l'AWSInfrastructure et les ressources IAM spécifiées dans un modèle de AWS CloudFormation chaîne d'outils. Le projet gère vos ressources de chaîne d'outils pour générer et déployer votre code source.

AWS CodeStar utilise AWS CloudFormation pour générer et déployer votre exemple de code. Cet exemple de code crée un service Web hébergé dans Amazon API Gateway AWS Lambda et accessible via Amazon API Gateway.

Prérequis :

- Suivez les étapes de [Configuration AWS CodeStar](#).
- Vous devez avoir créé un compartiment de stockage Amazon S3. Dans ce didacticiel, vous allez charger l'exemple de code source et le modèle de chaîne d'outils dans cet emplacement.

Note

Des coûts liés à ce didacticiel peuvent être facturés sur votre compte AWS, ce qui inclut l'utilisation des services AWS par AWS CodeStar. Pour plus d'informations, consultez [AWS CodeStar Pricing](#) (Tarification CTlong).

Rubriques

- [Étape 1 : Téléchargement et examen de l'exemple de code source](#)
- [Étape 2 : Téléchargement de l'exemple de modèle de chaîne d'outils](#)
- [Étape 3 : Test de votre modèle de chaîne d'outils dans AWS CloudFormation](#)
- [Étape 4 : Chargement de votre code source et de votre modèle de chaîne d'outils](#)
- [Étape 5 : Création d'un projet dans AWS CodeStar](#)

Étape 1 : Téléchargement et examen de l'exemple de code source

Dans le cadre de ce didacticiel, un fichier .zip est disponible en téléchargement. Il contient un exemple de code source pour un [exemple d'application](#) Node.js sur la plateforme de calcul Lambda. Lorsque le code source est placé dans votre référentiel, son dossier et ses fichiers se présentent comme suit :

```
tests/  
app.js  
buildspec.yml  
index.js  
package.json  
README.md  
template.yml
```

Les éléments de projet ci-dessous sont représentés dans votre exemple de code source :

- `tests/` : tests unitaires configurés pour le projet CodeBuild de ce projet. Ce dossier est inclus dans l'exemple de code, mais il n'est pas nécessaire à la création d'un projet.
- `app.js` : code source d'application de votre projet.
- `buildspec.yml` : instructions de génération pour l'étape de génération de votre ressource CodeBuild. Ce fichier est nécessaire pour un modèle de chaîne d'outils de modèle assorti d'une ressource CodeBuild .

- `package.json` : informations sur les dépendances de votre code source d'application.
- `README.md` : fichier readme de projet inclus dans tous les projets AWS CodeStar. Ce fichier est inclus dans l'exemple de code, mais il n'est pas nécessaire à la création d'un projet.
- `template.yml` : fichier de modèle d'infrastructure ou fichier de modèle SAM inclus dans tous les projets AWS CodeStar. Il est différent du fichier `template.yml` de chaîne d'outils que vous chargerez par la suite dans ce didacticiel. Ce fichier est inclus dans l'exemple de code, mais il n'est pas nécessaire à la création d'un projet.

Étape 2 : Téléchargement de l'exemple de modèle de chaîne d'outils

L'exemple de modèle de chaîne d'outils fourni pour ce didacticiel crée un référentiel (CodeCommit), un pipeline (CodePipeline) et un conteneur de génération (CodeBuild) et se sert de AWS CloudFormation pour déployer votre code source sur une plateforme Lambda. Outre ces ressources, il existe également des rôles IAM que vous pouvez utiliser pour définir les autorisations de votre environnement d'exécution, un compartiment Amazon S3 CodePipeline utilisé pour stocker vos artefacts de déploiement et une règle d'événements CloudWatch utilisée pour déclencher des déploiements de pipeline lorsque vous envoyez du code à votre référentiel. Pour vous conformer aux [bonnes pratiques AWS IAM](#), définissez les stratégies de vos rôles de chaîne d'outils définis dans cet exemple.

Téléchargez et décompressez l'exemple de modèle AWS CloudFormation au format [YAML](#).

Lorsque vous exécutez la commande `create-project` plus loin dans ce didacticiel, ce modèle créera les ressources de chaîne d'outils personnalisées suivantes dans AWS CloudFormation. Pour plus d'informations sur les ressources créées dans ce didacticiel, consultez les rubriques suivantes dans le [AWS CloudFormationGuide de l'utilisateur](#) :

- La [AWS::CodeCommit::Repository](#) AWS CloudFormationressource crée un CodeCommit référentiel.
- La [AWS::CodeBuild::Project](#) AWS CloudFormationressource crée un projet de CodeBuild construction.
- La [AWS::CodeDeploy::Application](#) AWS CloudFormationressource crée une CodeDeploy application.
- La [AWS::CodePipeline::Pipeline](#) AWS CloudFormationressource crée un CodePipeline pipeline.
- La [AWS::S3::Bucket](#) AWS CloudFormationressource crée le compartiment d'artefacts de votre pipeline.

- La [AWS::S3::BucketPolicy](#) AWS CloudFormation ressource crée la politique de compartiment d'artefacts pour le compartiment d'artefacts de votre pipeline.
- La [AWS::IAM::Role](#) AWS CloudFormation ressource crée le rôle de travailleur CodeBuild IAM qui donne AWS CodeStar les autorisations nécessaires pour gérer votre projet de CodeBuild construction.
- La [AWS::IAM::Role](#) AWS CloudFormation ressource crée le rôle de travailleur CodePipeline IAM qui donne AWS CodeStar les autorisations nécessaires pour créer votre pipeline.
- La [AWS::IAM::Role](#) AWS CloudFormation ressource crée le rôle de travailleur AWS CloudFormation IAM qui donne AWS CodeStar les autorisations nécessaires pour créer votre pile de ressources.
- La [AWS::IAM::Role](#) AWS CloudFormation ressource crée le rôle de travailleur AWS CloudFormation IAM qui donne AWS CodeStar les autorisations nécessaires pour créer votre pile de ressources.
- La [AWS::IAM::Role](#) AWS CloudFormation ressource crée le rôle de travailleur AWS CloudFormation IAM qui donne AWS CodeStar les autorisations nécessaires pour créer votre pile de ressources.
- La [AWS::Events::Rule](#) AWS CloudFormation ressource crée la règle CloudWatch Events qui surveille votre référentiel pour détecter les événements push.
- La [AWS::IAM::Role](#) AWS CloudFormation ressource crée le rôle CloudWatch Events IAM.

Étape 3 : Test de votre modèle de chaîne d'outils dans AWS CloudFormation

Avant de charger votre modèle de chaîne d'outils, vous pouvez le tester dans AWS CloudFormation et résoudre les erreurs éventuelles.

1. Enregistrez le modèle mis à jour sur votre ordinateur local, puis ouvrez la console AWS CloudFormation. Sélectionnez Create Stack (Créer une pile). Vos nouvelles ressources doivent figurer dans la liste.
2. Examinez votre pile pour voir si elle contient des erreurs de création de pile.
3. Une fois le test terminé, supprimez la pile.

Note

Veillez à supprimer votre pile et toutes les ressources créées dans AWS CloudFormation. Sinon, pendant que vous créez votre projet, vous pouvez rencontrer des erreurs liées à des noms de ressources déjà utilisés.

Étape 4 : Chargement de votre code source et de votre modèle de chaîne d'outils

Pour créer un AWS CodeStar projet, vous devez d'abord empaqueter votre code source dans un fichier .zip et le placer dans Amazon S3. AWS CodeStar initialise votre dépôt avec ce contenu. Vous spécifiez cet emplacement dans votre fichier d'entrée au moment d'exécuter la commande permettant de créer votre projet dans l'AWS CLI.

Vous devez également charger votre `toolchain.yml` fichier et le placer dans Amazon S3. Vous spécifiez cet emplacement dans votre fichier d'entrée au moment d'exécuter la commande permettant de créer votre projet dans l'AWS CLI.

Pour charger votre code source et votre modèle de chaîne d'outils

1. L'exemple de structure de fichiers suivante illustre les fichiers source et le modèle de chaîne d'outils prêts à être compressés et chargés. L'exemple de code inclut le fichier `template.yml`. Ne perdez pas de vue que ce fichier est différent du fichier `toolchain.yml`.

```
ls
src toolchain.yml

ls src/
README.md    app.js        buildspec.yml  index.js      package.json
template.yml  tests
```

2. Créez le fichier .zip pour les fichiers de code source.

```
cd src; zip -r "../src.zip" *; cd ../
```

3. Utilisez la `cp` commande et incluez les fichiers en tant que paramètres.

Les commandes suivantes chargent le fichier `.zip` `toolchain.yml` vers Amazon S3.

```
aws s3 cp src.zip s3://MyBucket/src.zip
aws s3 cp toolchain.yml s3://MyBucket/toolchain.yml
```

Pour configurer votre compartiment Amazon S3 afin de partager votre code source

- Comme vous stockez votre code source et votre chaîne d'outils dans Amazon S3, vous pouvez utiliser les politiques de compartiment Amazon S3 et les ACL d'objets pour garantir que les autres utilisateurs ou AWS comptes IAM puissent créer des projets à partir de vos exemples. AWS CodeStar garantit que tout utilisateur qui crée un projet personnalisé a accès à la chaîne d'outils et à la source qu'il souhaite utiliser.

Pour permettre à quiconque d'utiliser votre exemple, exécutez les commandes suivantes :

```
aws s3api put-object-acl --bucket MyBucket --key toolchain.yml --acl public-read
aws s3api put-object-acl --bucket MyBucket --key src.zip --acl public-read
```

Étape 5 : Création d'un projet dans AWS CodeStar

Pour créer votre projet, effectuez ces étapes.

Important

Assurez-vous de configurer la AWS région préférée dans AWS CLI. Votre projet est créé dans la AWS région configurée dans le AWS CLI.

1. Exécutez la commande `create-project` et incluez le paramètre `--generate-cli-skeleton` :

```
aws codestar create-project --generate-cli-skeleton
```

Des données au format JSON apparaissent dans la sortie. Copiez les données dans un fichier (par exemple, `input.json`) à un emplacement sur votre ordinateur local ou sur l'instance où est installée l'AWS CLI. Modifiez les données copiées comme suit, puis enregistrez vos résultats. Ce fichier d'entrée est configuré pour un projet nommé `MyProject` avec le nom de compartiment `myBucket`.

- Veillez à spécifier le paramètre `roleArn`. Pour les modèles personnalisés, comme l'exemple de modèle utilisé dans ce didacticiel, vous devez fournir un rôle. Ce rôle doit disposer d'autorisations pour créer toutes les ressources spécifiées dans [Étape 2 : Téléchargement de l'exemple de modèle de chaîne d'outils](#).

- Veillez à spécifier le paramètre `ProjectId` sous `stackParameters`. L'exemple de modèle fourni pour ce didacticiel a besoin de ce paramètre.

```
{
  "name": "MyProject",
  "id": "myproject",
  "description": "Sample project created with the CLI",
  "sourceCode": [
    {
      "source": {
        "s3": {
          "bucketName": "MyBucket",
          "bucketKey": "src.zip"
        }
      },
      "destination": {
        "codeCommit": {
          "name": "myproject"
        }
      }
    }
  ],
  "toolchain": {
    "source": {
      "s3": {
        "bucketName": "MyBucket",
        "bucketKey": "toolchain.yml"
      }
    },
    "roleArn": "role_ARN",
    "stackParameters": {
      "ProjectId": "myproject"
    }
  }
}
```

2. Placez-vous dans le répertoire contenant le fichier que vous venez d'enregistrer, puis exécutez à nouveau la commande `create-project`. Incluez le paramètre `--cli-input-json`.

```
aws codestar create-project --cli-input-json file://input.json
```

3. En cas de réussite, des données similaires à ce qui suit s'affichent dans la sortie :

```
{
  "id": "project-ID",
  "arn": "arn"
}
```

- La sortie contient des informations sur le nouveau projet :
 - La valeur de `id` représente l'ID du projet.
 - La valeur de `arn` représente l'ARN du projet.

4. Utilisez la commande `describe-project` pour vérifier le statut de votre création de projet. Incluez le paramètre `--id`.

```
aws codestar describe-project --id <project_ID>
```

Des données similaires à celles qui suivent s'affichent dans la sortie :

```
{
  "name": "MyProject",
  "id": "myproject",
  "arn": "arn:aws:codestar:us-east-1:account_ID:project/myproject",
  "description": "",
  "createdTimeStamp": 1539700079.472,
  "stackId": "arn:aws:cloudformation:us-east-1:account_ID:stack/awscodestar-myproject/stack-ID",
  "status": {
    "state": "CreateInProgress"
  }
}
```

- La sortie contient des informations sur le nouveau projet :
 - La valeur de `id` représente l'ID unique du projet.
 - La valeur de `state` représente le statut de création du projet, par exemple `CreateInProgress` ou `CreateComplete`.

Bien que votre projet soit en cours de création, vous pouvez [ajouter des membres de l'équipe](#) ou [configurer l'accès](#) à votre référentiel de projet à partir de la ligne de commande ou de votre IDE préféré.

Tutoriel : créer un projet de compétence Alexa dans AWS CodeStar

AWS CodeStar est un service de développement basé sur le cloud AWS qui fournit les outils dont vous avez besoin pour développer, créer et déployer rapidement des applications. Avec AWS CodeStar, vous pouvez configurer toute votre chaîne d'outils de livraison continue en quelques minutes et commencer à publier du code plus rapidement. Les modèles de projets de compétences Alexa AWS CodeStar ci-dessous vous permettent de créer une compétence Hello World Alexa simple à partir de votre AWS compte en quelques clics. Les modèles créent également un pipeline de déploiement de base qui vous permet de démarrer avec un flux de travail d'intégration continue (CI) pour le développement de compétences.

Les principaux avantages de la création de compétences Alexa AWS CodeStar sont que vous pouvez vous lancer dans le développement des compétences AWS et connecter votre compte de développeur Amazon au projet pour déployer les compétences directement depuis la phase de développement AWS. Vous bénéficiez également d'un pipeline (CI) de déploiement prêt à l'emploi, avec un référentiel contenant tout le code source pour le projet. Vous pouvez configurer ce référentiel avec votre environnement de développement intégré (IDE) favori afin de créer des compétences avec des outils que vous connaissez.

Prérequis

- Créez un compte de développeur Amazon en accédant à la page <https://developer.amazon.com>. L'inscription est gratuite. Ce compte est propriétaire de vos compétences Alexa.
- Si vous n'avez pas de compte AWS, suivez la procédure suivante pour en créer un.

Pour s'inscrire à AWS

1. Ouvrez <https://aws.amazon.com/>, puis choisissez Create an AWS Account.

Note

Si vous vous êtes déjà connecté à la AWS Management Console à l'aide d'informations d'identification Utilisateur racine d'un compte AWS, choisissez Sign in to a different account (Se connecter à un autre compte). Si vous vous êtes déjà connecté à la console à l'aide des informations d'identification IAM, choisissez Se connecter à l'aide Utilisateur racine d'un compte AWS des informations d'identification. Ensuite, choisissez Créer un nouveau compte AWS.

2. Suivez les instructions en ligne.

Important

Une fois que vous avez créé le projet de compétence Alexa, apportez toutes les modifications requises uniquement dans le référentiel du projet. Nous vous recommandons de ne pas modifier cette compétence directement à l'aide d'un autre outil du kit ASK (Alexa Skills Kit), tel que l'interface de ligne de commande ou la console du développeur ASK. Ces outils ne sont pas intégrés au référentiel du projet. Si vous les utilisez, les codes de la compétence et du référentiel ne seront plus synchronisés.

Étape 1 : Créer le projet et vous connecter à votre compte de développeur Amazon

Dans ce didacticiel, vous créez une compétence à l'aide de Node.js s'exécutant sur AWS Lambda. La plupart des étapes sont identiques pour les autres langages, mais le nom de la compétence diffère. Pour connaître les détails du modèle de projet que vous choisissez, reportez-vous au fichier README.md, situé dans le référentiel du projet.

1. Connectez-vous à la AWS CodeStar console AWS Management Console, puis ouvrez-la à l'adresse <https://console.aws.amazon.com/codestar/>.
2. Choisissez la région AWS dans laquelle vous souhaitez créer le projet et ses ressources. L'environnement d'exécution des compétences Alexa est disponible dans les AWS régions suivantes :
 - Asie Pacifique (Tokyo)
 - UE (Irlande)
 - USA Est (Virginie du Nord)
 - USA Ouest (Oregon)
3. Sélectionnez Create a project (Créer un projet).
4. Sur la page Choisir un modèle de projet :
 - a. Pour le type d'application, choisissez Alexa Skill.
 - b. Pour Langage de programmation, choisissez Node.js.
5. Choisissez la case qui contient vos sélections.

6. Pour Nom du projet, entrez un nom pour le projet (par exemple, **My Alexa Skill**). Si vous utilisez un autre nom, veillez à l'utiliser tout au long de ce didacticiel. AWS CodeStar choisit un identifiant associé pour ce projet comme identifiant de projet (par exemple, my-alexa-skill). Si un ID de projet différent vous est proposé, veillez à l'utiliser tout au long de ce didacticiel.
7. Choisissez AWS CodeCommit pour le référentiel dans ce didacticiel et ne modifiez pas la valeur du nom du référentiel.
8. Choisissez Connect Amazon developer account (Connecter un compte de développeur Amazon) pour pouvoir héberger la compétence sur votre compte de développeur Amazon. Si vous n'avez pas de compte de développeur Amazon, créez-en un et complétez d'abord l'enregistrement auprès d'[Amazon Developers](#).
9. Connectez-vous avec vos informations d'identification de développeur Amazon. Choisissez Autoriser, puis Confirmer pour terminer la connexion.
10. Si plusieurs ID fournisseur sont associés à votre compte de développeur Amazon, choisissez celui que vous souhaitez utiliser pour ce projet. Veillez à utiliser un compte auquel le rôle Administrateur ou Développeur a été attribué.
11. Choisissez Suivant.
12. (Facultatif) S'il s'agit de votre première utilisation AWS CodeStar dans cette AWS région, entrez le nom d'affichage et l'adresse e-mail que vous souhaitez utiliser pour votre utilisateur IAM. Choisissez Suivant.
13. Attendez qu'AWS CodeStar crée le projet. Cela peut prendre plusieurs minutes. Ne poursuivez pas tant que vous n'avez pas vu la bannière de provisionnement du projet.

Étape 2 : Tester votre compétence dans le simulateur Alexa

À la première étape, AWS CodeStar a créé une compétence pour vous et l'a déployée vers la phase de développement de compétence Alexa. Vous allez maintenant tester la compétence dans le simulateur Alexa.

1. Dans votre projet dans la AWS CodeStar console, choisissez Afficher l'application. Le simulateur Alexa s'ouvre dans un nouvel onglet.
2. Connectez-vous avec les informations d'identification du compte de développeur Amazon que vous avez utilisé à l'étape 1.
3. Sous Test (Tester), choisissez Development (Développement) pour activer les tests.
4. Saisissez `ask hello node hello`. Le nom d'appel par défaut pour votre compétence est `hello node`.

5. Votre compétence doit répondre Hello World!

Lorsque la compétence est activée dans le simulateur Alexa, vous pouvez également l'appeler sur un appareil Alexa enregistré sur votre compte de développeur Amazon. Pour tester votre compétence sur un appareil, dites : « Alexa, demande à hello node de dire bonjour ».

Pour plus d'informations sur le simulateur Alexa, consultez [Test Your Skill in the Developer Console \(Tester votre compétence dans la console des développeurs\)](#).

Étape 3 : Parcourir les ressources du projet

Dans le cadre de la création du projet, vous AWS CodeStar avez également créé AWS des ressources en votre nom. Ces ressources incluent un référentiel de projets utilisant CodeCommit, un pipeline de déploiement utilisant CodePipeline et une AWS Lambda fonction. Vous pouvez accéder à ces ressources à partir de la barre de navigation. Par exemple, le choix de Repository affiche des détails sur le CodeCommit référentiel. Vous pouvez consulter l'état du déploiement du pipeline sur la page Pipeline. Vous pouvez consulter la liste complète des AWS ressources créées dans le cadre de votre projet en choisissant Vue d'ensemble dans la barre de navigation. Cette liste comprend des liens vers chaque ressource.

Étape 4 : Modifier la réponse de votre compétence

Au cours de cette étape, vous apportez une légère modification à la réponse de votre compétence pour comprendre le cycle d'itération.

1. Dans la barre de navigation, choisissez Repository. Cliquez sur le lien sous Nom du référentiel et le référentiel de votre projet s'ouvre dans un nouvel onglet ou une nouvelle fenêtre. Ce référentiel contient la spécification de génération (buildspec.yml), la pile d'applications (template.yml) AWS CloudFormation, le fichier readme et le code source de votre compétence dans le [format de package de compétences \(structure du projet\)](#).
2. Accédez au fichier lambda > custom (personnalisé) > index.js (si Node.js est utilisé). Ce fichier contient votre code de gestion des demandes, qui utilise le [Kit de développement logiciel \(SDK\) ASK](#).
3. Choisissez Edit (Modifier).
4. Remplacez la chaîne Hello World! de la ligne 24 par la chaîne Hello. How are you?
5. Faites défiler jusqu'à la fin du fichier. Saisissez le nom de l'auteur et l'adresse e-mail ainsi qu'un message de validation éventuel.

6. Choisissez Commit changes (Valider les modifications) pour valider les modifications dans le référentiel.
7. Retournez au projet AWS CodeStar et consultez la page Pipeline. Vous devriez désormais voir le pipeline en cours de déploiement.
8. Lorsque le déploiement du pipeline est terminé, testez à nouveau votre compétence dans le simulateur Alexa. Elle devrait désormais répondre Hello. How are you?

Étape 5 : Configurer votre poste de travail local pour qu'il se connecte à votre référentiel de projet

Plus tôt, vous avez apporté une petite modification au code source directement depuis la CodeCommit console. Au cours de cette étape, vous configurez le référentiel du projet et votre poste de travail local pour pouvoir modifier et gérer le code à partir de la ligne de commande ou de votre IDE préféré. Les étapes suivantes expliquent comment configurer les outils de ligne de commande.

1. Accédez au tableau de bord du projet dans AWS CodeStar, si nécessaire.
2. Dans la barre de navigation, choisissez IDE.
3. Dans Accédez au code de votre projet, affichez les instructions sous l'interface de ligne de commande.
4. Suivez les instructions pour réaliser les tâches suivantes :
 - a. Installez Git sur votre poste de travail local à partir d'un site web tel que [Git Downloads](#).
 - b. Installez la CLI AWS. Pour plus d'informations, consultez [Installation de l'interface de ligne de commande AWS](#).
 - c. Configurez la AWS CLI avec votre clé d'accès utilisateur IAM et votre clé secrète. Pour plus d'informations, consultez [la section Configuration de la AWS CLI](#).
 - d. Clonez le CodeCommit dépôt du projet sur votre poste de travail local. Pour plus d'informations, consultez la section [Connect to a CodeCommit Repository](#).

Étapes suivantes

Ce didacticiel vous a montré comment développer une compétence de base. Pour approfondir la question, consultez les ressources suivantes.

- Découvrez les principes fondamentaux d'une compétence en regardant [How Alexa Skills Work](#) et d'autres vidéos sur la YouTube chaîne Alexa Developers.

- Comprenez les différents composants de votre compétence en passant en revue la documentation relative au [format de package de compétences](#), aux [schémas de manifestes de compétences](#) et aux [schémas de modèles d'interactions](#).
- Transformez votre idée en compétence en passant en revue la documentation relative à l'[Alexa Skills Kit](#) et aux [kits de développement logiciel \(SDK\) ASK](#).

Tutoriel : Création d'un projet avec un référentiel GitHub source

Vous pouvez ainsi configurer votre référentiel pour créer, examiner et fusionner des pull requests avec votre équipe de projet. AWS CodeStar

Dans ce didacticiel, vous allez créer un projet avec un exemple de code source d'application Web dans un GitHub référentiel, un pipeline qui déploie vos modifications et des instances EC2 où votre application est hébergée dans le cloud. Une fois votre projet créé, ce didacticiel explique comment créer et fusionner une GitHub pull request qui modifie la page d'accueil de votre application Web.

Rubriques

- [Étape 1 : Création du projet et création de votre GitHub référentiel](#)
- [Étape 2 : Afficher votre code source](#)
- [Étape 3 : créer une GitHub pull request](#)

Étape 1 : Création du projet et création de votre GitHub référentiel


Au cours de cette étape, utilisez la console pour créer votre projet et créer une connexion à votre nouveau GitHub référentiel. Pour accéder à votre GitHub référentiel, vous créez une ressource de connexion qui AWS CodeStar permet de gérer les autorisations avec GitHub. Lorsque le projet est créé, ses ressources supplémentaires sont mises à votre disposition.

1. Connectez-vous à la AWS CodeStar console AWS Management Console, puis ouvrez-la à l'adresse <https://console.aws.amazon.com/codestar/>.
2. Choisissez la région AWS dans laquelle vous souhaitez créer le projet et ses ressources.
3. Sur la AWS CodeStar page, choisissez Créer un projet.
4. Sur la page Choisir un modèle de projet, cochez les cases Application Web, Node.js et Amazon EC2. Ensuite, choisissez parmi les modèles disponibles pour cet ensemble d'options.

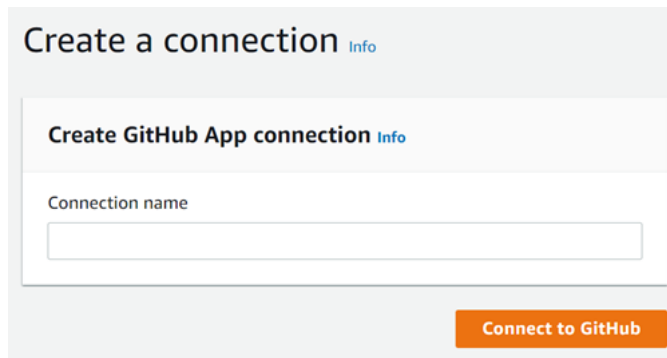
Pour plus d'informations, veuillez consulter [Modèles de projet AWS CodeStar](#).

5. Choisissez Suivant.
6. Pour Nom du projet, entrez un nom pour le projet (par exemple, **MyTeamProject**). Si vous utilisez un autre nom, veillez à l'utiliser tout au long de ce didacticiel.
7. Sous Référentiel de projets, choisissez GitHub.
8. Si vous le souhaitez GitHub, vous devrez choisir ou créer une ressource de connexion. Si vous avez déjà une connexion, sélectionnez-la dans le champ de recherche. Dans le cas contraire, vous allez créer une nouvelle connexion ici. Choisissez Connect to GitHub.

La page Créer une connexion s'affiche.

 Note


Pour créer une connexion, vous devez disposer d'un GitHub compte. Si vous créez une connexion pour une organisation, vous devez en être le propriétaire.



- a. Sous Créer une connexion à GitHub l'application, dans Nom de la connexion, entrez le nom de votre connexion. Choisissez Connect to GitHub.


La GitHub page Connect to affiche et affiche le champ GitHub Applications.

- b. 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.


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

 Note

Si vous avez déjà installé l'application, vous pouvez choisir Configurer (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.

- d. Si la page Confirmer le mot de passe pour continuer s'affiche, entrez votre GitHub mot de passe, puis choisissez Se connecter.
- e. Sur la GitHub page Installer le AWS connecteur pour, laissez les valeurs par défaut et choisissez Installer.
- f. Sur la GitHub page Connect to, l'ID d'installation de votre nouvelle installation apparaît dans GitHubApps.

Une fois la connexion créée avec succès, le message Ready to connect s'affiche sur la page de CodeStar création de projet.

 Note

Vous pouvez consulter votre connexion dans les paramètres de la console Developer Tools. Pour plus d'informations, voir [Commencer à utiliser les connexions](#).

Select a repository provider

CodeCommit
Use a new AWS CodeCommit repository for your project.

GitHub
Use a new GitHub source repository for your project (requires an existing GitHub account).

The GitHub repository provider now uses CodeStar Connections
To use a GitHub repository in CodeStar, create a connection. The connection will use GitHub Apps to access your repository. Use the following options to choose an existing connection or create a new one. [Learn more](#)

Connection
Choose an existing connection or create a new one and then return to this task.

am:aws:codestar-connections:us-east- X or **Connect to GitHub**

Ready to connect
Your Github connection is ready for use.

Repository owner
The owner of the new repository. This can be a personal GitHub account or a GitHub organization.

Repository name
The name of the new repository.

Repository description
An optional description of the new repository.

Public

- g. Pour Propriétaire du référentiel, choisissez l' GitHuborganisation ou votre GitHub compte personnel.
- h. Pour Nom du référentiel, acceptez le nom du GitHub référentiel par défaut ou saisissez-en un autre.
- i. Choisissez Public ou Privé.

Note

Si vous souhaitez l'utiliser AWS Cloud9 comme environnement de développement, vous devez choisir un dépôt public.

- j. (Facultatif) Dans Description du référentiel, entrez une description pour le GitHub référentiel.

9. Configurez vos instances Amazon EC2 dans Configuration Amazon EC2 si votre projet est déployé sur des instances Amazon EC2 et que vous souhaitez apporter des modifications. Par exemple, vous pouvez choisir des types d'instances disponibles pour votre projet.

Dans Key pair, choisissez la paire de clés Amazon EC2 que vous avez créée dans. [Étape 4 : Création d'une paire de clés Amazon EC2 pour les projets AWS CodeStar](#) Sélectionnez Je reconnais avoir accès au fichier de clé privée.

10. Choisissez Suivant.
11. Examinez les ressources et les détails de configuration.
12. Choisissez Suivant ou Créer un projet. (Le choix affiché dépend de votre modèle de projet.)

Attendez quelques minutes pendant la création de votre projet.

13. Une fois votre projet créé, choisissez Afficher l'application pour afficher votre application Web.

Étape 2 : Afficher votre code source

Au cours de cette étape, vous visualisez votre code source et les outils que vous pouvez utiliser pour votre référentiel de sources.

1. Dans la barre de navigation de votre projet, choisissez Repository.

Pour afficher la liste des validations dans GitHub, choisissez Afficher les validations. Cela ouvre l'historique de vos validations dans GitHub.

Pour consulter les problèmes, choisissez l'onglet Problèmes correspondant à votre projet. Pour créer un nouveau problème dans GitHub, choisissez Créer un GitHub problème. Cela ouvre le formulaire de demande de dépôt dans GitHub.

2. Dans l'onglet Référentiel, cliquez sur le lien sous Nom du référentiel, et le référentiel de votre projet s'ouvre dans un nouvel onglet ou une nouvelle fenêtre. Ce dépôt contient le code source de votre projet.

Étape 3 : créer une GitHub pull request

Au cours de cette étape, vous apportez une modification mineure à votre code source et créez une pull request.

1. Dans GitHub, créez une nouvelle branche de fonctionnalités dans votre référentiel. Choisissez le champ déroulant de la branche principale et entrez une nouvelle branche dans le champ nommé `feature-branch`. Choisissez Créer une nouvelle branche. La succursale est créée et extraite pour vous.
2. Dans GitHub, apportez une modification dans la `feature-branch` branche. Ouvrez le dossier public et ouvrez le `index.html` fichier.
3. Dans la AWS CodeStar console, sous Pull requests, pour créer une pull request dans GitHub, choisissez Create pull request. Cela ouvre le formulaire de pull request de votre dépôt dans GitHub. Dans GitHub, choisissez l'icône en forme de crayon pour modifier le fichier.

Ensuite Congratulations!, ajoutez la chaîne Well done, <name>! et remplacez-la <name> par votre nom. Choisissez Valider les modifications. La modification est validée dans votre branche de fonctionnalités.

4. Dans la AWS CodeStar console, choisissez votre projet. Choisissez l'onglet Référentiel. Sous Pull requests, choisissez Create pull request.

Le formulaire s'ouvre dans GitHub. Laissez la branche principale dans la branche de base. Pour Comparer à, choisissez votre branche de fonctionnalités. Afficher le diff.

5. Dans GitHub, choisissez Create pull request. Une pull request nommée Update index.html est créée.
6. Dans la AWS CodeStar console, consultez la nouvelle pull request. Choisissez Fusionner les modifications pour valider les modifications dans le référentiel et fusionner la pull request avec la branche principale de votre référentiel.
7. Retournez au projet AWS CodeStar et consultez la page Pipeline. Vous devriez désormais voir le pipeline en cours de déploiement.
8. Une fois votre projet créé, choisissez Afficher l'application pour afficher votre application Web.

Modèles de projet AWS CodeStar

AWS CodeStar les modèles de projet vous permettent de commencer par un exemple d'application et de le déployer à l'aide AWS des ressources créées pour soutenir votre projet de développement. Lorsque vous choisissez un modèle de AWS CodeStar projet, le type d'application, le langage de programmation et la plate-forme de calcul sont configurés pour vous. Une fois que vous avez créé des projets avec des applications web, des services web, des compétences Alexa et des pages web statiques, vous pouvez remplacer l'exemple d'application par votre propre application.

Après avoir AWS CodeStar créé votre projet, vous pouvez modifier les AWS ressources qui prennent en charge la livraison de votre application. AWS CodeStar fonctionne avec AWS CloudFormation pour vous permettre d'utiliser du code pour créer des services de support et des serveurs/plateformes sans serveur dans le cloud. AWS CloudFormation vous permet de modéliser l'ensemble de votre infrastructure dans un fichier texte.

Rubriques

- [Fichiers et ressources de projet AWS CodeStar](#)
- [Mise en route : Choix d'un modèle de projet](#)
- [Comment procéder pour modifier votre projet AWS CodeStar](#)

Fichiers et ressources de projet AWS CodeStar

Un projet AWS CodeStar rassemble le code source et les ressources créées pour déployer le code. Les ressources qui, ensemble, aident à générer, publier et déployer le code sont appelées ressources de chaîne d'outils. Lors de la création d'un projet, un modèle AWS CloudFormation alloue les ressources de chaîne d'outils dans un pipeline d'intégration continue/de déploiement continu (CI/CD).

Vous pouvez l'utiliser AWS CodeStar pour créer des projets de deux manières, en fonction de votre niveau d'expérience en matière de création de AWS ressources :

- Lorsque vous utilisez la console pour créer un projet, AWS CodeStar crée vos ressources de chaîne d'outils, y compris votre référentiel, et remplit ce dernier avec des exemples de code d'application et de fichiers de projet. Utilisez la console pour configurer rapidement des exemples de projets à partir d'un ensemble d'options de projet préconfigurées.

- Lorsque vous utilisez l'interface de ligne de commande pour créer un projet, vous devez fournir le modèle AWS CloudFormation créant vos ressources de chaîne d'outils et le code source de l'application. Utilisez l'interface de ligne de commande pour permettre à AWS CodeStar de créer votre projet à partir de votre modèle, puis remplissez votre référentiel avec vos exemples de code.

Un projet AWS CodeStar fournit un seul point de gestion. Vous pouvez utiliser l'assistant Créer un projet dans la console pour configurer un exemple de projet. Vous pouvez ensuite l'utiliser comme plateforme de collaboration pour la gestion des autorisations et des ressources de votre équipe. Pour plus d'informations, veuillez consulter [Qu'est-ce qu'AWS CodeStar ?](#). Lorsque vous utilisez la console pour créer un projet, votre code source est fourni sous forme d'exemple de code et vos ressources de chaîne d'outils CI/CD sont créées pour vous.

Lorsque vous créez un projet dans la console, AWS CodeStar alloue les ressources suivantes :

- Un référentiel de code dans GitHub ou CodeCommit.
- Dans le référentiel de projet, un fichier README .md qui fournit les détails des fichiers et des annuaires.
- Dans le référentiel de projet, un fichier `template.yml` qui stocke la définition de la pile d'exécution de votre application. Vous utilisez ce fichier pour ajouter ou modifier des ressources de projet qui ne sont pas des ressources de chaîne d'outils, telles que les AWS ressources utilisées pour les notifications, le support de base de données, la surveillance et le suivi.
- AWS les services et ressources créés en relation avec votre pipeline, tels que le compartiment d'artefacts Amazon S3, Amazon CloudWatch Events et les rôles de service associés.
- Un exemple d'application opérationnel avec le code source complet et un point de terminaison HTTP public.
- Une ressource AWS de calcul, basée sur le type de modèle de AWS CodeStar projet :
 - Une fonction Lambda.
 - Une instance Amazon EC2.
 - Un environnement AWS Elastic Beanstalk.
- À partir du 6 décembre 2018 PDT :
 - Une limite d'autorisations qui est une stratégie IAM spécialisée pour contrôler l'accès aux ressources du projet. La limite d'autorisations est attachée par défaut à des rôles dans l'exemple de projet. Pour de plus amples informations, veuillez consulter [Limite d'autorisations IAM pour les rôles de travail](#).

- Un rôle AWS CloudFormation IAM permettant de créer des ressources de projet à l'aide duquel AWS CloudFormation inclut des autorisations pour toutes les ressources AWS CloudFormation prises en charge, y compris les rôles IAM.
- Un rôle de chaîne de compilation IAM.
- Les rôles d'exécution pour Lambda sont définis dans la pile d'applications, que vous pouvez modifier.
- Avant le 6 décembre 2018 PDT :
 - Un rôle AWS CloudFormation IAM pour créer des ressources de projet prenant en charge un ensemble limité de ressources AWS CloudFormation.
 - Rôle IAM pour créer une CodePipeline ressource.
 - Rôle IAM pour créer une CodeBuild ressource.
 - Rôle IAM pour créer une CodeDeploy ressource, s'il est applicable à votre type de projet.
 - Un rôle IAM pour créer l'application Web Amazon EC2, le cas échéant, à votre type de projet.
 - Rôle IAM pour créer une ressource d' CloudWatch événements.
 - Rôle d'exécution pour Lambda qui est modifié dynamiquement pour inclure un ensemble partiel de ressources.

Le projet inclut des pages détaillées qui indiquent le statut et contiennent des liens vers la gestion de l'équipe, des liens vers des instructions de configuration pour les IDE ou votre référentiel, ainsi qu'un historique des validations des modifications du code source dans le référentiel. Vous pouvez également sélectionner des outils pour la connexion à des outils externes de suivi des problèmes, tels que Jira.

Mise en route : Choix d'un modèle de projet

Lorsque vous choisissez un projet AWS CodeStar dans la console, vous effectuez votre choix parmi un ensemble d'options préconfigurées avec un exemple de code et des ressources vous permettant de faire vos premiers pas rapidement. Ces options sont appelés modèles de projet. Chaque modèle de AWS CodeStar projet comprend un langage de programmation, un type d'application et une plateforme de calcul. La combinaison que vous sélectionnez détermine le modèle de projet.

Choix d'une plateforme de calcul de modèle

Chaque modèle configure l'un des types de plateformes de calcul suivants :

- Lorsque vous choisissez un AWS Elastic Beanstalk projet, vous le déployez dans un AWS Elastic Beanstalk environnement sur des instances Amazon Elastic Compute Cloud dans le cloud.
- Lorsque vous choisissez un projet Amazon EC2, vous AWS CodeStar créez des instances Linux EC2 pour héberger votre application dans le cloud. Les membres de votre équipe de projet peuvent accéder aux instances, et votre équipe utilise la paire de clés que vous fournissez pour accéder par SSH à vos instances Amazon EC2. AWS CodeStar dispose également d'un SSH géré qui utilise les autorisations des membres de l'équipe pour gérer les connexions par paires de clés.
- Lorsque vous le AWS Lambda souhaitez, AWS CodeStar crée un environnement sans serveur accessible via Amazon API Gateway, sans instance ni serveur à gérer.

Choix d'un type d'application de modèle

Chaque modèle configure l'un des types d'applications suivants :

- Service web

Un service web est utilisé pour les tâches qui s'exécutent en arrière-plan, telles que les appels d'API. Une fois qu'AWS CodeStar a créé votre exemple de projet de service web, vous pouvez choisir l'URL du point de terminaison pour voir la sortie « Hello World », mais la principale utilisation de ce type d'application n'est pas l'utilisation comme interface utilisateur. Les modèles de projet AWS CodeStar de cette catégorie prennent en charge le développement en Ruby, Java, ASP.NET, PHP, Node.js et autres.

- Application web

Une application web fonctionne comme une interface utilisateur. Une fois qu'AWS CodeStar a créé votre exemple de projet d'application web, vous pouvez choisir l'URL du point de terminaison pour afficher une application web interactive. Les modèles de projet AWS CodeStar de cette catégorie prennent en charge le développement en Ruby, Java, ASP.NET, PHP, Node.js et autres.

- Page web statique

Choisissez ce modèle si vous souhaitez un projet pour un site web HTML. Les modèles de projet AWS CodeStar de cette catégorie prennent en charge le développement en HTML5.

- Compétence Alexa

Choisissez ce modèle si vous souhaitez un projet pour une compétence Alexa avec une fonction AWS Lambda. Lorsque vous créez le projet de compétence, AWS CodeStar renvoie un Amazon

Resource Name (ARN) que vous pouvez utiliser comme point de terminaison de service. Pour plus d'informations, voir [Héberger une compétence personnalisée en tant que fonction AWS Lambda](#).

Note

Les fonctions Lambda pour les compétences Alexa ne sont prises en charge que dans les régions USA Est (Virginie du Nord), USA Ouest (Oregon), UE (Irlande) et Asie-Pacifique (Tokyo).

- Règle de configuration

Choisissez ce modèle si vous souhaitez créer un projet de AWS Config règle qui vous permette d'automatiser les règles entre les AWS ressources de votre compte. La fonction renvoie un ARN que vous pouvez utiliser comme point de terminaison de service pour votre règle.

Choix d'un langage de programmation de modèle

Lorsque vous choisissez un modèle de projet, vous sélectionnez un langage de programmation, tel que Ruby, Java, ASP.NET, PHP, Node.js, ou autre.

Comment procéder pour modifier votre projet AWS CodeStar

Vous pouvez mettre à jour votre projet en modifiant :

- L'exemple de code et les ressources de langage de programmation de votre application.
- Les ressources qui constituent l'infrastructure dans laquelle votre application est stockée et déployée (systèmes d'exploitation, applications et services de support, paramètres de déploiement et plateforme de calcul du cloud). Vous pouvez modifier les ressources de l'application dans le fichier `template.yml`. Il s'agit du fichier AWS CloudFormation qui modélise l'environnement d'exécution de votre application.

Note

Si vous travaillez sur un AWS CodeStar projet Alexa Skills, vous ne pouvez pas modifier la compétence en dehors du référentiel AWS CodeStar source (CodeCommit ou GitHub). Si

vous modifiez la compétence Alexa sur le portail des développeurs, la modification pourra ne pas être visible dans le référentiel source et les deux versions seront désynchronisées.

Modification du code source de l'application et transmission des modifications

Pour modifier un exemple de code source, des scripts et d'autres fichiers source de l'application, modifiez les fichiers dans votre référentiel source comme suit :

- En utilisant le mode Édition dans CodeCommit ou GitHub.
- Ouvrez le projet dans un environnement IDE, tel qu'AWS Cloud9.
- Clonez le référentiel localement, puis validez et transmettez vos modifications. Pour plus d'informations, consultez [Étape 4 : valider une modification](#).

Modifier les ressources de l'application à l'aide du fichier Template.yml

Au lieu de modifier manuellement une ressource d'infrastructure, utilisez AWS CloudFormation pour modéliser et déployer les ressources d'exécution de votre application.

Vous pouvez modifier ou ajouter une ressource d'application, telle qu'une fonction Lambda, dans votre pile d'exécution en modifiant le fichier `template.yml` dans votre référentiel de projet. Vous pouvez ajouter toute ressource qui est disponible en tant que ressource AWS CloudFormation.

Pour modifier le code ou les paramètres d'une fonction AWS Lambda, consultez [Ajout d'une ressource à un projet](#).

Modifiez le fichier `template.yml` dans le référentiel de votre projet en ajoutant le type des ressources AWS CloudFormation qui sont des ressources d'application. Lorsque vous ajoutez une ressource d'application à la section `Resources` du fichier `template.yml`, AWS CloudFormation et AWS CodeStar créent la ressource pour vous. Pour obtenir la liste des AWS CloudFormation ressources et leurs propriétés requises, consultez la section [Référence AWS des types de ressources](#). Pour plus d'informations, consultez cet exemple dans [Étape 1 : Modifier le rôle du CloudFormation travailleur dans IAM](#).

AWS CodeStar vous permet de mettre en œuvre les bonnes pratiques en configurant et en modélisant l'environnement d'exécution de votre application.

Comment gérer les autorisations de modification des ressources d'application

Lorsque vous utilisez AWS CloudFormation pour ajouter des ressources d'application d'exécution, telles que la fonction Lambda, le rôle de travail AWS CloudFormation peut utiliser les autorisations qu'il possède déjà. Pour certaines ressources d'application d'exécution, vous devez ajuster manuellement les autorisations du rôle de travail AWS CloudFormation pour pouvoir modifier le fichier `template.yml`.

Pour obtenir un exemple de modification des autorisations du rôle de travail AWS CloudFormation, consultez [Étape 5 : ajouter des autorisations de ressources avec une stratégie en ligne](#).

Bonnes pratiques AWS CodeStar

AWS CodeStar est intégré à plusieurs produits et services. Les sections suivantes décrivent les bonnes pratiques pour AWS CodeStar et pour ces produits et services connexes.

Rubriques

- [Bonnes pratiques de sécurité pour les ressources AWS CodeStar](#)
- [Bonnes pratiques en matière de définition des versions de dépendances](#)
- [Surveillance et journalisation des bonnes pratiques pour les ressources AWS CodeStar](#)

Bonnes pratiques de sécurité pour les ressources AWS CodeStar

Vous devez appliquer régulièrement des correctifs et examiner les bonnes pratiques en matière de sécurité pour les dépendances utilisées par votre application. Servez-vous de ces bonnes pratiques de sécurité pour mettre à jour votre exemple de code et maintenir votre projet dans un environnement de production :

- Suivez les annonces et les mises à jour continues de sécurité pour votre infrastructure.
- Avant de déployer votre projet, suivez les bonnes pratiques établies pour votre infrastructure.
- Examinez régulièrement les dépendances de votre infrastructure et procédez à des mises à jour, si nécessaire.
- Chaque modèle AWS CodeStar contient des instructions de configuration pour votre langage de programmation. Consultez le fichier README .md dans le référentiel source de votre projet.
- En tant que meilleure pratique pour isoler les ressources du projet, gérez l'accès aux ressources avec le moindre privilège à AWS l'aide d'une stratégie multi-comptes telle qu'introduite dans.

[Sécurité dans AWS CodeStar](#)

Bonnes pratiques en matière de définition des versions de dépendances

L'exemple de code source de votre projet AWS CodeStar utilise des dépendances qui sont répertoriées dans le fichier package .json de votre référentiel source. La bonne pratique consiste à toujours définir vos dépendances de telle sorte qu'elles pointent vers une version spécifique. C'est

ce que l'on appelle « épingler la version ». Nous vous déconseillons de définir la version sur `latest`, car les modifications qui peuvent être introduites sont susceptibles d'interrompre votre application sans préavis.

Surveillance et journalisation des bonnes pratiques pour les ressources AWS CodeStar

Vous pouvez utiliser les fonctions de journalisation de AWS pour déterminer les actions que les utilisateurs ont effectuées dans votre compte et les ressources utilisées. Les fichiers journaux affichent :

- La date et l'heure des actions
- L'adresse IP source d'une action
- Les actions qui ont échoué en raison d'autorisations inadéquates

AWS CloudTrail peut être utilisé pour enregistrer les appels AWS d'API et les événements connexes effectués par ou pour le compte d'un AWS compte. Pour plus d'informations, veuillez consulter [Journalisation des AWS CodeStar appels d'API avec AWS CloudTrail](#).

Utilisation des projets dans AWS CodeStar

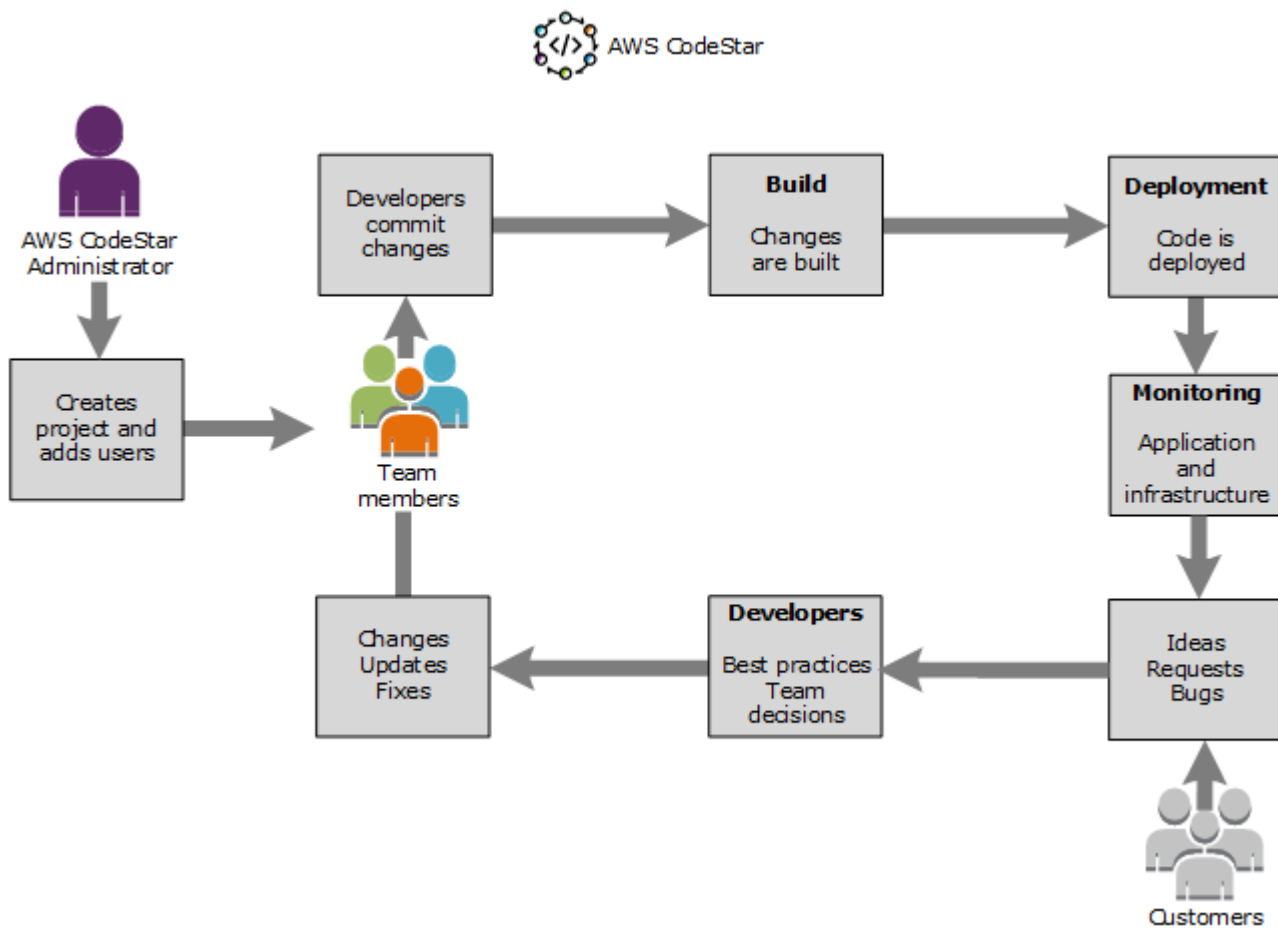
Lorsque vous utilisez un modèle de AWS CodeStar projet, vous pouvez créer rapidement un projet déjà configuré avec les ressources dont vous avez besoin, notamment :

- Référentiel source
- Environnement de build
- Ressources de déploiement et d'hébergement
- Langage de programmation

Le modèle inclut même un exemple de code source, afin que vous puissiez utiliser immédiatement votre projet.

Une fois que vous disposez d'un projet, vous pouvez ajouter ou supprimer des ressources, personnaliser le tableau de bord du projet et surveiller la progression.

Le schéma suivant illustre un flux de travail basique dans un projet AWS CodeStar.



Le flux de travail de base présenté dans le diagramme montre un développeur avec la `AWSCodeStarFullAccess` politique appliquée qui crée un projet et y ajoute des membres de l'équipe. Ensemble, ils écrivent, créent, testent et déploient du code. Le tableau de bord du projet fournit des outils qui peuvent être utilisés en temps réel pour afficher l'activité de l'application et surveiller les builds, le flux du code dans le pipeline de déploiement, etc. L'équipe utilise sa vignette Team wiki pour partager des informations, des bonnes pratiques et des liens. Elle intègre son logiciel de suivi des problèmes pour faciliter le suivi de la progression et des tâches. À mesure que les clients fournissent des demandes et des commentaires en retour, l'équipe ajoute ces informations au projet tout en les intégrant à la planification et au développement de leur projet. À mesure que le projet se développe, l'équipe ajoute des membres de l'équipe supplémentaires afin de prendre en charge leur base de code.

Créer un projet dans AWS CodeStar

Vous utilisez la console AWS CodeStar pour créer un projet. Si vous utilisez un modèle de projet, ce dernier configure les ressources nécessaires à votre place. Ce modèle comprend également un exemple de code que vous pouvez utiliser pour commencer le codage.

Pour créer un projet, connectez-vous au AWS Management Console avec un utilisateur IAM disposant de la `AWSCodeStarFullAccess` politique ou d'autorisations équivalentes. Pour plus d'informations, veuillez consulter [Configuration AWS CodeStar](#).

Note

Vous devez suivre les étapes décrites dans cette rubrique [Configuration AWS CodeStar](#) avant de pouvoir exécuter les procédures décrites dans cette rubrique.

Rubriques

- [Créer un projet dans AWS CodeStar \(Console\)](#)
- [Créer un projet dans AWS CodeStar \(AWS CLI\)](#)

Créer un projet dans AWS CodeStar (Console)

Utilisez la console AWS CodeStar pour créer un projet.

Pour créer un projet dans AWS CodeStar

1. Connectez-vous à la AWS CodeStar consoleAWS Management Console, puis ouvrez-la à l'adresse <https://console.aws.amazon.com/codestar/>.

Vérifiez que vous êtes connecté à la région AWS dans laquelle vous souhaitez créer le projet et ses ressources. Par exemple, pour créer un projet dans l'est des États-Unis (Ohio), assurez-vous d'avoir sélectionné cette AWS région. Pour plus d'informations sur les régions AWS dans lesquelles AWS CodeStar est disponible, consultez [Régions et points de terminaison](#) dans le document Référence générale AWS.

2. Sur la AWS CodeStarpage, choisissez Créer un projet.
3. Sur la page Choisir un modèle de projet, choisissez le type de projet dans la liste des modèles de AWS CodeStar projet. Vous pouvez utiliser la barre de filtre pour affiner vos choix. Par


exemple, pour un projet d'application Web écrit dans Node.js à déployer sur des instances Amazon EC2, cochez les cases Application Web, Node.js et Amazon EC2. Ensuite, choisissez parmi les modèles disponibles pour cet ensemble d'options.

Pour plus d'informations, veuillez consulter [Modèles de projet AWS CodeStar](#).

4. Choisissez Suivant.
5. Dans le champ de saisie du nom du projet, entrez un nom pour le projet, tel que *Mon premier projet*. Dans Project ID, l'ID du projet est dérivé du nom du projet, mais il est limité à 15 caractères.

Par exemple, l'ID par défaut d'un projet nommé *Mon premier projet* est *my-first-projec*. Cet identifiant de projet est à la base des noms de toutes les ressources associées au projet. AWS CodeStar utilise cet ID de projet dans l'URL de votre référentiel de code et pour les noms des rôles et politiques d'accès de sécurité associés dans IAM. Une fois le projet créé, l'ID de projet ne peut pas être modifié. Pour modifier l'ID de projet avant de créer le projet, dans ID de projet, entrez l'ID que vous souhaitez utiliser.


Pour plus d'informations sur les limites des noms de projet et des ID de projet, consultez [Limites dans AWS CodeStar](#).

 Note

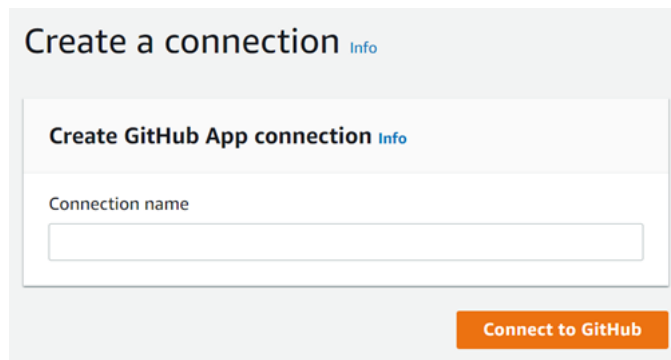
Les ID de projet doivent être uniques pour votre compte AWS dans une région AWS.

6. Choisissez le fournisseur de référentiel, AWS CodeCommit ou GitHub.
7. Si vous avez choisi AWS CodeCommit, dans Nom du référentiel, acceptez le nom de référentiel AWS CodeCommit par défaut ou entrez-en un différent. Passez ensuite à l'étape 9.
8. Si vous le souhaitez GitHub, vous devez choisir ou créer une ressource de connexion. Si vous avez déjà une connexion, sélectionnez-la dans le champ de recherche. Dans le cas contraire, créez une nouvelle connexion dès maintenant. Choisissez Connect to GitHub.

La page Créer une connexion s'affiche.

 Note

Pour créer une connexion, vous devez disposer d'un GitHub compte. Si vous créez une connexion pour une organisation, vous devez en être le propriétaire.



The screenshot shows a web interface for creating a connection. At the top, it says "Create a connection" with a small "Info" link. Below that, there's a section titled "Create GitHub App connection" also with an "Info" link. Underneath is a text input field labeled "Connection name". At the bottom right of this section is an orange button that says "Connect to GitHub".

- a. Sous Créer une connexion à GitHub l'application, dans le champ de saisie du nom de la connexion, entrez le nom de votre connexion. Choisissez Connect to GitHub.

La GitHub page Connect to affiche et affiche le champ GitHub Applications.

- b. 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.


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

Note

Si vous avez déjà installé l'application, vous pouvez choisir Configurer (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.


- d. Si la page Confirmer le mot de passe pour continuer s'affiche, entrez votre GitHub mot de passe, puis choisissez Se connecter.
- e. Sur la GitHub page Installer le AWS connecteur pour, conservez les valeurs par défaut et choisissez Installer.

- g. Pour Propriétaire du référentiel, choisissez l' GitHub organisation ou votre GitHub compte personnel.
- h. Pour Nom du référentiel, acceptez le nom du GitHub référentiel par défaut ou saisissez-en un autre.
- i. Choisissez Public ou Privé.

 Note


Pour l'utiliser AWS Cloud9 comme environnement de développement, vous devez sélectionner Public.

- j. (Facultatif) Dans Description du référentiel, entrez une description pour le GitHub référentiel.

 Note

Si vous choisissez un modèle de projet Alexa Skill, vous devez connecter un compte développeur Amazon. Pour plus d'informations sur l'utilisation des projets Alexa Skill, consultez [Tutoriel : créer un projet de compétence Alexa dans AWS CodeStar](#).

- 9. Si votre projet est déployé sur des instances Amazon EC2 et que vous souhaitez apporter des modifications, configurez vos instances Amazon EC2 dans Configuration Amazon EC2. Par exemple, vous pouvez choisir des types d'instances disponibles pour votre projet.

 Note

Les différents types d'instances Amazon EC2 fournissent différents niveaux de puissance de calcul et peuvent entraîner des coûts associés différents. Pour plus d'informations, consultez les [types d'instances Amazon EC2 et les tarifs Amazon EC2](#). Si vous avez plusieurs clouds privés virtuels (VPC) ou plusieurs sous-réseaux créés dans Amazon Virtual Private Cloud, vous pouvez également choisir le VPC et le sous-réseau à utiliser. Toutefois, si vous choisissez un type d'instance Amazon EC2 qui n'est pas pris en charge sur les instances dédiées, vous ne pouvez pas choisir un VPC dont la location d'instance est définie sur Dedicated. Pour plus d'informations, consultez [Qu'est-ce qu'Amazon VPC ?](#) et les [bases des instances dédiées](#).

Dans Key pair, choisissez la paire de clés Amazon EC2 que vous avez créée dans. [Étape 4 : Création d'une paire de clés Amazon EC2 pour les projets AWS CodeStar](#) Sélectionnez Je reconnais avoir accès au fichier de clé privée.

10. Choisissez Suivant.
11. Examinez les ressources et les détails de configuration.
12. Choisissez Suivant ou Créer un projet. (Le choix affiché dépend de votre modèle de projet.)

La création du projet, y compris du référentiel, peut prendre quelques minutes.

13. Une fois que votre projet dispose d'un référentiel, vous pouvez utiliser la page Référentiel pour configurer l'accès à celui-ci. Utilisez les liens des étapes suivantes pour configurer un IDE, configurer le suivi des problèmes ou ajouter des membres de l'équipe à votre projet.

Bien que votre projet soit en cours de création, vous pouvez [ajouter des membres de l'équipe](#) ou [configurer l'accès](#) à votre référentiel de projet à partir de la ligne de commande ou de votre IDE préféré.

Créer un projet dans AWS CodeStar (AWS CLI)


Un projet AWS CodeStar rassemble le code source et les ressources créées pour déployer le code. Les ressources qui, ensemble, aident à générer, publier et déployer le code sont appelées ressources de chaîne d'outils. Lors de la création d'un projet, un modèle AWS CloudFormation alloue les ressources de chaîne d'outils dans un pipeline d'intégration continue/de déploiement continu (CI/CD).

Lorsque vous utilisez la console pour créer un projet, le modèle de chaîne d'outils est créé pour vous. Lorsque vous utilisez l'AWS CLI pour créer un projet, vous créez le modèle de chaîne d'outils qui génère vos ressources de chaîne d'outils.

Une chaîne d'outils complète nécessite les ressources recommandées suivantes :

1. Un CodeCommit GitHub référentiel contenant votre code source.
2. Un CodePipeline pipeline configuré pour écouter les modifications apportées à votre dépôt.
 - a. Lorsque vous exécutez CodeBuild des tests unitaires ou d'intégration, nous vous recommandons d'ajouter une phase de construction à votre pipeline afin de créer des artefacts de construction.

- b. Nous vous recommandons d'ajouter à votre pipeline une étape de déploiement qui utilise CodeDeploy ou qui permet de AWS CloudFormation déployer votre artefact de build et votre code source sur votre infrastructure d'exécution.

 Note

Dans la mesure où un pipeline CodePipeline nécessite au moins deux étapes et que la première étape doit être l'étape source, ajoutez une étape de construction ou de déploiement comme deuxième étape.

AWS CodeStar les chaînes d'outils sont définies sous forme de [CloudFormation modèle](#).

Pour accéder à un didacticiel qui présente cette tâche et qui configure des exemples de ressources, consultez [Didacticiel : Création d'un projet dans AWS CodeStar à l'aide de l'AWS CLI](#).

Prérequis :

Lorsque vous créez un projet, vous fournissez les paramètres suivants dans un fichier d'entrée. Si les éléments suivants ne sont pas définis, AWS CodeStar crée un projet vide.

- Code source. Si ce paramètre est présent dans la demande, vous devez également inclure un modèle de chaîne d'outils.
 - Votre code source doit contenir le code d'application nécessaire à l'exécution de votre projet.
 - Votre code source doit inclure tous les fichiers de configuration requis, tels qu'un `buildspec.yml` pour un CodeBuild projet ou un `appspect.yml` pour un déploiement. CodeDeploy
 - Vous pouvez inclure des éléments facultatifs dans votre code source, tels qu'un fichier `README` ou un `template.yml` pour les ressources autres que la chaîne d'outils. AWS
- Modèle de chaîne d'outils. Votre modèle de chaîne d'outils fournit les AWS ressources et les rôles IAM à gérer pour votre projet.
- Emplacements des sources. Si vous spécifiez le code source et un modèle de chaîne d'outils pour votre projet, vous devez préciser un emplacement. Téléchargez vos fichiers source et votre modèle de chaîne d'outils dans le compartiment Amazon S3. AWS CodeStar récupère les fichiers et les utilise pour créer le projet.

⚠ Important

Assurez-vous de configurer la AWS région préférée dans leAWS CLI. Votre projet est créé dans la AWS région configurée dans leAWS CLI.

1. Exécutez la commande `create-project` et incluez le paramètre `--generate-cli-skeleton` :

```
aws codestar create-project --generate-cli-skeleton
```

Des données au format JSON apparaissent dans la sortie. Copiez les données dans un fichier (par exemple, `input.json`) à un emplacement sur votre ordinateur local ou sur l'instance où est installée l'AWS CLI. Modifiez les données copiées comme suit, puis enregistrez vos résultats.

```
{
  "name": "project-name",
  "id": "project-id",
  "description": "description",
  "sourceCode": [
    {
      "source": {
        "s3": {
          "bucketName": "s3-bucket-name",
          "bucketKey": "s3-bucket-object-key"
        }
      },
      "destination": {
        "codeCommit": {
          "name": "codecommit-repository-name"
        },
        "gitHub": {
          "name": "github-repository-name",
          "description": "github-repository-description",
          "type": "github-repository-type",
          "owner": "github-repository-owner",
          "privateRepository": true,
          "issuesEnabled": true,
          "token": "github-personal-access-token"
        }
      }
    }
  ]
}
```

```
    ],
    "toolchain": {
      "source": {
        "s3": {
          "bucketName": "s3-bucket-name",
          "bucketKey": "s3-bucket-object-key"
        }
      },
      "roleArn": "service-role-arn",
      "stackParameters": {
        "KeyName": "key-name"
      }
    },
    "tags": {
      "KeyName": "key-name"
    }
  }
}
```

Remplacez les éléments suivants :

- *nom-projet* : obligatoire. Nom descriptif pour ce projet AWS CodeStar.
- *id-projet* : obligatoire. Identifiant de projet pour ce projet AWS CodeStar.

Note


Vous devez attribuer un identifiant de projet unique lorsque vous créez un projet. Une erreur s'affiche si vous soumettez un fichier d'entrée avec un identifiant de projet qui existe déjà.

- *description* : facultatif. Description de ce projet AWS CodeStar.
- *codeSource* : facultatif. Informations de configuration pour le code source fourni pour le projet. Actuellement, un seul objet `sourceCode` est pris en charge. Chaque objet `sourceCode` contient des informations sur l'emplacement dans lequel le code source est extrait par AWS CodeStar et sur la destination où le code source est renseigné.
- *source* : obligatoire. Définit l'emplacement dans lequel vous avez chargé votre code source. La seule source prise en charge est Amazon S3. AWS CodeStar récupère le code source et l'inclut dans le référentiel après la création de votre projet.
 - *S3* : facultatif. L'emplacement de votre code source sur Amazon S3.
 - *nom-compartiment* : compartiment contenant votre code source.

- *clé-compartiment* : préfixe de compartiment et clé d'objet qui pointent vers le fichier .zip contenant votre code source (par exemple, src.zip).
- *destination* : facultatif. Emplacements de destination où votre code source doit être renseigné lors de la création du projet. Les destinations prises en charge pour votre code source sont CodeCommit et GitHub.


Vous pouvez fournir uniquement l'une des deux options suivantes :

- *CodeCommit* : le seul attribut obligatoire est le nom CodeCommit du dépôt qui doit contenir votre code source. Ce référentiel doit se trouver dans votre modèle de chaîne d'outils.

 Note

En CodeCommit effet, vous devez fournir le nom du référentiel que vous avez défini dans votre pile de chaînes d'outils. AWS CodeStar initialise ce référentiel avec le code source que vous avez fourni dans Amazon S3.


- *GitHub* : cet objet représente les informations requises pour créer le GitHub référentiel et l'ensemencer avec le code source. Si vous choisissez un GitHub référentiel, les valeurs suivantes sont obligatoires.

 Note

En effet GitHub, vous ne pouvez pas spécifier un GitHub référentiel existant. AWS CodeStar en crée un pour vous et remplit ce référentiel avec le code source que vous avez chargé sur Amazon S3. AWS CodeStar utilise les informations suivantes pour créer votre référentiel dans GitHub.

- *nom* : obligatoire. Le nom de votre GitHub dépôt.
- *description* : obligatoire. Description de votre GitHub dépôt.
- *type* : obligatoire. Type de GitHub référentiel. Les valeurs valides sont Utilisateur ou Organisation.
- *propriétaire* : obligatoire. Le nom GitHub d'utilisateur du propriétaire de votre dépôt. Si le référentiel doit appartenir à une GitHub organisation, indiquez le nom de l'organisation.


- **référentielPrivé** : obligatoire. Indique si vous souhaitez que ce référentiel soit privé ou public. Les valeurs valides sont vrai (true) ou faux (false).
- **problèmesActivés** : obligatoire. Si vous souhaitez activer les problèmes liés GitHub à ce référentiel. Les valeurs valides sont vrai (true) ou faux (false).
- **jeton** : facultatif. Il s'agit d'un jeton d'accès personnel AWS CodeStar utilisé pour accéder à votre GitHub compte. Ce jeton doit contenir les règles suivantes : repo, user et admin:repo_hook. Pour récupérer un jeton d'accès personnel GitHub, voir [Création d'un jeton d'accès personnel pour la ligne de commande](#) sur le GitHub site Web.

 Note

Si vous utilisez la CLI pour créer un projet avec un référentiel GitHub source, utilisez votre jeton pour accéder au référentiel via des AWS CodeStar applications OAuth. Si vous utilisez la console pour créer un projet avec un référentiel GitHub source, AWS CodeStar utilise une ressource de connexion qui accède au référentiel avec des GitHub applications.

- **chaîne d'outils** : informations concernant la chaîne d'outils CI/CD à configurer lors de la création du projet. Emplacement dans lequel vous avez téléchargé le modèle de chaîne d'outils. Ce modèle crée la pile AWS CloudFormation contenant vos ressources de chaîne d'outils. Il s'agit également d'éventuels remplacements de paramètres qu'AWS CloudFormation doit référencer et du rôle à utiliser pour créer la pile. AWS CodeStar extrait le modèle et utilise AWS CloudFormation pour l'exécuter.
- **source** : obligatoire. L'emplacement de votre modèle de chaîne d'outils. Amazon S3 est le seul emplacement source pris en charge.
 - **S3** : facultatif. L'emplacement Amazon S3 où vous avez chargé votre modèle de chaîne d'outils.
 - **bucket-name** : nom du compartiment Amazon S3.
 - **clé-compartiment** : préfixe de compartiment et clé d'objet qui pointent vers le fichier .yaml ou .json contenant votre modèle de chaîne d'outils (par exemple, files/toolchain.yaml).
 - **paramètresPile** : facultatif. Contient les paires clé-valeur à transmettre à AWS CloudFormation. Il s'agit des paramètres, le cas échéant, que votre modèle de chaîne d'outils doit référencer, s'il est configuré pour.

- **rôle** : facultatif. Rôle utilisé pour créer vos ressources de chaîne d'outils dans votre compte. Le rôle est requis comme suit :
 - Si le rôle n'est pas fourni, AWS CodeStar utilise le rôle de service par défaut créé pour votre compte si la chaîne d'outils est un modèle quickstart AWS CodeStar. Si le rôle de service n'existe pas dans votre compte, vous pouvez en créer un. Pour plus d'informations, consultez [Étape 2 : créer le rôle AWS CodeStar de service](#).
 - Vous devez fournir le rôle si vous chargez et utilisez votre propre modèle de chaîne d'outils personnalisés. Vous pouvez créer un rôle en fonction du rôle de service AWS CodeStar et de sa déclaration de stratégie. Pour obtenir un exemple de cette déclaration de stratégie, veuillez consulter [AWSCodeStarServiceRole Politique](#).
- **balises** : facultatif. Balises attachées à votre projet AWS CodeStar.

 Note

Ces balises ne sont pas attachées aux ressources contenues dans le projet.

2. Placez-vous dans le répertoire contenant le fichier que vous venez d'enregistrer, puis exécutez à nouveau la commande `create-project`. Incluez le paramètre `--cli-input-json`.

```
aws codestar create-project --cli-input-json file://input.json
```

3. En cas de réussite, des données similaires à ce qui suit s'affichent dans la sortie :

```
{
  "id": "project-ID",
  "arn": "arn"
}
```

- La sortie contient des informations sur le nouveau projet :
 - La valeur de `id` représente l'ID du projet.
 - La valeur de `arn` représente l'ARN du projet.
4. Utilisez la commande `describe-project` pour vérifier le statut de votre création de projet. Incluez le paramètre `--id`.

```
aws codestar describe-project --id <project_ID>
```

Des données similaires à celles qui suivent s'affichent dans la sortie :

```
{
  "name": "MyProject",
  "id": "myproject",
  "arn": "arn:aws:codestar:us-east-1:account_ID:project/myproject",
  "description": "",
  "createdTimeStamp": 1539700079.472,
  "stackId": "arn:aws:cloudformation:us-east-1:account_ID:stack/awscodestar-
myproject/stack-ID",
  "status": {
    "state": "CreateInProgress"
  }
}
```

- La sortie contient des informations sur le nouveau projet :
 - La valeur de `state` représente le statut de création du projet, par exemple `CreateInProgress` ou `CreateComplete`.

Bien que votre projet soit en cours de création, vous pouvez [ajouter des membres de l'équipe](#) ou [configurer l'accès](#) à votre référentiel de projet à partir de la ligne de commande ou de votre IDE préféré.

Utilisation d'un IDE avec AWS CodeStar

Lorsque vous intégrez un environnement de développement intégré (IDE) avec AWS CodeStar, vous pouvez continuer à écrire et développer du code dans votre environnement préféré. Les modifications que vous apportez sont incluses dans le projet AWS CodeStar chaque fois que vous validez et transmettez votre code en mode push.

The screenshot shows an IDE interface with a code editor on the left and a Git commit interface on the right. The code editor displays the following HTML code:

```

48     <nav class="website-nav">
49         <ul>
50             <li><a class="home-link" href="https://aws.amazon.com/">
51             <li><a href="https://aws.amazon.com/what-is-cloud-comput
52             <li><a href="https://aws.amazon.com/solutions/">Services
53             <li><a href="https://aws.amazon.com/contact-us/">Contact
54         </ul>
55     </nav>
56 </header>
57
58     <div class="message">
59         <a class="twitter-link" href="http://twitter.com/home/?status=I
60         <div class="text">
61             <h1>Congratulations!</h1>
62             <h2>You just created a Node.js web application</h2>
63             <h3>And I made a change in Eclipse!</h3>
64         </div>
65     </div>
66 </div>
67
68     <footer>
69         <p class="footer-contents">Designed and developed with <a href="http

```

The Git commit interface shows the following details:

- Project: **my-first-projec [master]**
- Unstaged Changes (1): `.project`
- Staged Changes (1): `index.html - public`
- Commit Message: `Updated index.html with a new h3`
- Author: `Mary Major <mary_major@example.com>`
- Committer: `Mary Major <mary_major@example.com>`
- Buttons: `Commit and Push...` and `Commit`

Rubriques

- [Utiliser AWS Cloud9 avec AWS CodeStar](#)
- [Utilisation d'Eclipse avec AWS CodeStar](#)
- [Utilisez Visual Studio avec AWS CodeStar](#)

Utiliser AWS Cloud9 avec AWS CodeStar

Vous pouvez utiliser AWS Cloud9 pour effectuer des modifications de code et développer des logiciels dans un projet AWS CodeStar. AWS Cloud9 est un IDE en ligne, auquel vous pouvez accéder via votre navigateur web. L'IDE offre une expérience d'édition de code enrichie : il prend en

charge plusieurs langages de programmation et débogueurs d'exécution, et comporte un terminal intégré. En arrière-plan, une instance Amazon EC2 héberge un environnement de AWS Cloud9 développement. Cet environnement fournit l'IDE AWS Cloud9 et l'accès aux fichiers de code du projet AWS CodeStar. Pour plus d'informations, consultez le [AWS Cloud9 Guide de l'utilisateur](#).

Vous pouvez utiliser la console AWS CodeStar ou AWS Cloud9 pour créer des environnements de développement AWS Cloud9 pour les projets qui stockent leur code dans CodeCommit. Pour les AWS CodeStar projets dans lesquels leur code est stocké GitHub, vous ne pouvez utiliser que la AWS Cloud9 console. Cette rubrique décrit comment utiliser les deux consoles.

Pour utiliser AWS Cloud9, vous avez besoin des éléments suivants :

- Un utilisateur IAM qui a été ajouté à un projet AWS CodeStar en tant que membre de l'équipe.
- Si le AWS CodeStar projet enregistre son code source dans les AWS informations CodeCommit d'identification de l'utilisateur IAM.

Rubriques

- [Création d'un environnement AWS Cloud9 pour un projet](#)
- [Ouverture d'un environnement AWS Cloud9 pour un projet](#)
- [Partage d'un environnement AWS Cloud9 avec un membre de l'équipe de projet](#)
- [Suppression d'un environnement AWS Cloud9 d'un projet](#)
- [À utiliser GitHub avec AWS Cloud9](#)
- [Ressources supplémentaires](#)

Création d'un environnement AWS Cloud9 pour un projet

Suivez ces étapes pour créer un environnement de développement AWS Cloud9 pour un projet AWS CodeStar.

1. Suivez les étapes ci-dessous [Créer un projet](#) si vous souhaitez créer un nouveau projet.
2. Ouvrez le projet dans la console AWS CodeStar. Dans la barre de navigation, choisissez IDE. Choisissez Créer un environnement, puis suivez les étapes ci-dessous.

⚠ Important

Si le projet se trouve dans une AWS région où il AWS Cloud9 n'est pas pris en charge, aucune AWS Cloud9 option ne s'affichera dans l'onglet IDE de la barre de navigation. Cependant, vous pouvez utiliser la console AWS Cloud9 pour créer un environnement de développement, ouvrir le nouvel environnement, puis le connecter au référentiel AWS CodeCommit du projet. Ignorez les étapes suivantes et consultez [Création d'un environnement](#), [Ouverture d'un environnement](#) et l'[Exemple AWS CodeCommit](#) dans le Guide de l'utilisateur AWS Cloud9. Pour obtenir la liste des régions AWS prises en charge, consultez [AWS Cloud9](#) dans le manuel Référence générale d'Amazon Web Services.

Dans Créer un AWS Cloud9 environnement, personnalisez les paramètres par défaut du projet.


1. Pour modifier le type par défaut d'instance Amazon EC2 afin d'héberger l'environnement, dans Type d'instance, choisissez le type d'instance.
2. AWS Cloud9 utilise Amazon Virtual Private Cloud (Amazon VPC) dans votre AWS compte pour communiquer avec l'instance. En fonction de la configuration d'Amazon VPC dans votre AWS compte, effectuez l'une des opérations suivantes.

Le compte a-t-il un VPC avec au moins un sous-réseau dans ce VPC ?	Est-ce le VPC que vous voulez qu'AWS Cloud9 utilise par défaut dans le compte ?	Le VPC a-t-il un seul sous-réseau ?	Faire ceci
Non	—	—	Si aucun VPC n'existe, créez-en un. Développez Paramètres réseau. Pour Network (VPC) (Réseau (VPC)), choisissez Créer VPC et suivez les instructions affichées sur la page. Pour plus d'informations,

Le compte a-t-il un VPC avec au moins un sous-réseau dans ce VPC ?	Est-ce le VPC que vous voulez qu'AWS Cloud9 utilise par défaut dans le compte ?	Le VPC a-t-il un seul sous-réseau ?	Faire ceci
			<p>consultez la section Créer un Amazon VPC pour AWS Cloud9 dans le guide de l'AWS Cloud9 utilisateur.</p> <p>Si un VPC existe mais n'a pas de sous-réseau, créez-en un. Développez Paramètres réseau. Pour Réseau (VPC), choisissez Créer le sous-réseau et suivez les instructions affichées sur la page. Pour plus d'informations, consultez Créer un sous-réseau au pour AWS Cloud9 dans le Guide de l'utilisateur AWS Cloud9.</p>
Oui	Oui	Oui	<p> Passez directement à l'étape 4 de cette procédure . (AWS Cloud9 utilise le VPC par défaut, avec son sous-réseau unique.)</p>
Oui	Oui	Non	<p>Pour Sous-réseau, choisissez le sous-réseau que vous voulez qu'AWS Cloud9 utilise dans le VPC par défaut présélectionné.</p>
Oui	Non	Oui ou Non	<p>Pour Réseau (VPC), choisissez le VPC que vous voulez qu'AWS Cloud9 utilise. Pour Sous-réseau, choisissez le sous-réseau que vous voulez qu'AWS Cloud9 utilise dans ce VPC.</p>

Pour plus d'informations, consultez les [paramètres Amazon VPC pour les environnements de AWS Cloud9 développement](#) dans le guide de l'utilisateur AWS Cloud9.

3. Entrez un nom d'environnement et ajoutez éventuellement une description de l'environnement.

 Note

Les noms d'environnement doivent être uniques pour chaque utilisateur.

4. Pour modifier la période par défaut après laquelle l'environnement AWS Cloud9 est arrêté lorsqu'il n'a pas été utilisé, développez les paramètres de réduction des coûts, puis modifiez le paramètre.
5. Choisissez Create environment.


Pour ouvrir l'environnement, consultez [Ouverture d'un environnement AWS Cloud9 pour un projet](#).

Vous pouvez utiliser ces étapes pour créer plusieurs environnements pour un projet. Par exemple, vous pouvez souhaiter utiliser un environnement pour travailler sur une partie du code et un autre environnement pour travailler sur la même partie du code avec des paramètres différents.

Ouverture d'un environnement AWS Cloud9 pour un projet

Suivez ces étapes pour ouvrir un environnement de développement AWS Cloud9 que vous avez créé pour un projet AWS CodeStar.

1. Le projet étant ouvert dans la AWS CodeStar console, dans la barre de navigation, choisissez IDE.

 Important

Si le code source du projet est stocké dans GitHub, vous ne verrez pas l'IDE dans la barre de navigation. Cependant, vous pouvez utiliser la console AWS Cloud9 pour ouvrir un environnement existant. Ignorez le reste de cette procédure et consultez [Ouverture d'un environnement](#) dans le Guide de l'utilisateur AWS Cloud9 et [À utiliser GitHub avec AWS Cloud9](#).

2. Pour Vos environnements AWS Cloud9 ou Environnements AWS Cloud9 partagés, choisissez Ouvrir l'IDE pour l'environnement à ouvrir.

Vous pouvez utiliser l'IDE AWS Cloud9 pour commencer tout de suite à utiliser du code dans le référentiel AWS CodeCommit du projet. Pour plus d'informations, consultez [La fenêtre d'environnement](#), [L'éditeur, les onglets et les volets](#) et [Le terminal](#) dans le Guide de l'utilisateur AWS Cloud9 et [Commandes Git de base](#) dans le Guide de l'utilisateur AWS CodeCommit.

Partage d'un environnement AWS Cloud9 avec un membre de l'équipe de projet

Une fois que vous avez créé un environnement de développement AWS Cloud9 pour un projet AWS CodeStar, vous pouvez inviter d'autres utilisateurs de votre compte AWS, y compris les membres de l'équipe de projet, à accéder à ce même environnement. Cela est particulièrement utile pour la programmation en binôme, où deux programmeurs codent et donnent des conseils tour à tour sur le même code par le biais du partage d'écran ou en étant assis au même poste de travail. Les membres de l'environnement peuvent utiliser l'IDE AWS Cloud9 partagé pour voir les modifications de code apportées par chaque membre mises en évidence dans l'éditeur de code et pour discuter avec d'autres membres pendant qu'ils effectuent du codage.

L'ajout d'un membre de l'équipe à un projet n'autorise pas automatiquement ce dernier à participer aux environnements de développement AWS Cloud9 associés du projet. Pour inviter un membre de l'équipe de projet à accéder à un environnement pour un projet, vous devez déterminer le rôle d'accès approprié pour le membre de l'environnement, appliquer des politiques AWS gérées à l'utilisateur et l'inviter dans votre environnement. Pour plus d'informations, consultez les sections [À propos des rôles d'accès des membres de l'environnement](#) et [Inviter un utilisateur IAM dans votre environnement](#) dans le guide de l'AWS Cloud9utilisateur.

Lorsque vous invitez un membre de l'équipe de projet à accéder à un environnement d'un projet, la console AWS CodeStar affiche l'environnement à ce membre de l'équipe. L'environnement est affiché dans la liste des environnements partagés de l'onglet IDE de la AWS CodeStar console du projet. Pour afficher cette liste, demandez au membre de l'équipe d'ouvrir le projet dans la console, puis de choisir IDE dans la barre de navigation.

Important

Si le code source du projet est stocké dans GitHub, vous ne verrez pas l'IDE dans la barre de navigation. Cependant, vous pouvez utiliser la console AWS Cloud9 pour inviter d'autres utilisateurs de votre compte AWS, y compris les membres de l'équipe de projet, à accéder à un environnement. Pour ce faire, consultez [À utiliser GitHub avec AWS Cloud9](#) ce guide, ainsi que les sections [À propos des rôles d'accès des membres de l'environnement](#) et [Inviter un utilisateur IAM dans votre environnement](#) dans le guide de l'AWS Cloud9utilisateur.

Vous pouvez également inviter un utilisateur qui n'est pas membre de l'équipe de projet à accéder à un environnement. Par exemple, vous pouvez souhaiter qu'un utilisateur puisse travailler sur le code d'un projet, mais sans avoir accès à ce projet. Pour inviter ce type d'utilisateur, reportez-vous aux sections [À propos des rôles d'accès des membres de l'environnement](#) et [Inviter un utilisateur IAM dans votre environnement](#) dans le guide de l'AWS Cloud9 utilisateur. Lorsque vous invitez un utilisateur qui n'est pas membre de l'équipe de projet à accéder à un environnement d'un projet, ce dernier peut utiliser la console AWS Cloud9 pour accéder à l'environnement. Pour plus d'informations, consultez [Ouverture d'un environnement](#) dans le Guide de l'utilisateur AWS Cloud9.

Suppression d'un environnement AWS Cloud9 d'un projet

Lorsque vous supprimez un projet et toutes ses ressources AWS d'AWS Cloud9, tous les environnements de développement AWS CodeStar associés qui ont été créés avec la console AWS CodeStar sont également supprimés et ne peuvent pas être récupérés. Vous pouvez supprimer un environnement de développement d'un projet sans supprimer le projet.

1. Le projet étant ouvert dans la AWS CodeStar console, dans la barre de navigation, choisissez IDE.

Important

Si le code source du projet est stocké dans GitHub, vous ne verrez pas l'IDE dans la barre de navigation. Cependant, vous pouvez utiliser la console AWS Cloud9 pour supprimer un environnement de développement. Ignorez le reste de cette procédure et consultez [Suppression d'un environnement](#) dans le Guide de l'utilisateur AWS Cloud9.

2. Choisissez l'environnement que vous souhaitez supprimer dans les environnements Cloud9 et choisissez Supprimer
3. Entrez **delete** pour confirmer la suppression pour l'environnement de développement, puis choisissez Supprimer.

Warning

Vous ne pouvez pas récupérer un environnement de développement après l'avoir supprimé. Toutes les modifications de code non enregistrées dans l'environnement sont perdues.

À utiliser GitHub avec AWS Cloud9

Pour les AWS CodeStar projets dont le code source est stocké GitHub, la AWS CodeStar console ne prend pas en charge l'utilisation directe des environnements de AWS Cloud9 développement. Cependant, vous pouvez utiliser la AWS Cloud9 console pour travailler avec le code source dans les GitHub référentiels.

1. Utilisez la console AWS Cloud9 pour créer un environnement de développement AWS Cloud9. Pour plus d'informations, consultez [Création d'un environnement](#) dans le Guide de l'utilisateur AWS Cloud9.
2. Utilisez la console AWS Cloud9 pour ouvrir l'environnement de développement. Pour plus d'informations, consultez [Ouverture d'un environnement](#) dans le Guide de l'utilisateur AWS Cloud9.
3. Dans l'IDE, utilisez une session de terminal pour vous connecter au GitHub référentiel (processus connu sous le nom de clonage). Si une session de terminal n'est pas en cours d'exécution, dans la barre de menus dans l'IDE, choisissez Window, New Terminal (Fenêtre, Nouveau terminal). Pour connaître les commandes à utiliser pour cloner le GitHub référentiel, consultez la section [Clonage d'un référentiel](#) sur le site Web d' GitHub aide.

Pour accéder à la page principale du GitHub référentiel, le projet étant ouvert dans la AWS CodeStar console, dans la barre de navigation latérale, sélectionnez Code.

4. Utilisez la fenêtre Environnement et les onglets de l'éditeur dans l'IDE pour afficher, modifier et enregistrer le code. Pour plus d'informations, consultez [La fenêtre d'environnement](#) et [L'éditeur, les onglets et les volets](#) dans le Guide de l'utilisateur AWS Cloud9.
5. Utilisez Git dans la session de terminal de l'IDE pour transmettre vos modifications de code au référentiel et extraire régulièrement les modifications de code des autres à partir du référentiel. Pour plus d'informations, consultez les [sections Transfert vers un référentiel distant et Récupération d'un référentiel distant](#) sur le GitHub site Web d'aide. Pour les commandes Git, consultez [Git Cheatsheet sur le site](#) Web d' GitHub aide.

Note

Pour empêcher Git de vous demander vos identifiants de GitHub connexion chaque fois que vous envoyez ou extrayez du code depuis le dépôt, vous pouvez utiliser un assistant d'identification. Pour plus d'informations, consultez la section [Mise en cache de votre GitHub mot de passe dans Git](#) sur le site Web GitHub d'aide.

Ressources supplémentaires

Pour plus d'informations sur l'utilisation d'AWS Cloud9, consultez ce qui suit dans le Guide de l'utilisateur AWS Cloud9 :

- [Didacticiel](#)
- [Utilisation des environnements](#)
- [Utilisation de l'IDE](#)
- [Exemples](#)

Utilisation d'Eclipse avec AWS CodeStar

Vous pouvez utiliser Eclipse pour apporter des modifications au code et développer des logiciels dans un AWS CodeStar projet. Vous pouvez modifier votre code de projet AWS CodeStar avec Eclipse, puis valider et transmettre vos modifications au référentiel source pour le projet AWS CodeStar.

Note

Les informations de cette section s'appliquent uniquement aux projets AWS CodeStar dont le code source est stocké dans CodeCommit. Si votre AWS CodeStar projet stocke son code source dans GitHub, vous pouvez utiliser un outil tel que eGit pour Eclipse. Pour plus d'informations, consultez la [documentation EGit](#) sur le site web EGit.

Si le AWS CodeStar projet stocke son code source dans CodeCommit, vous devez installer une version compatible avec AWS CodeStar. AWS Toolkit for Eclipse Vous devez également être un membre de l'équipe du projet AWS CodeStar disposant du rôle de propriétaire ou de participant.

Pour utiliser Eclipse, vous avez également besoin des éléments suivants :

- Un utilisateur IAM qui a été ajouté à un AWS CodeStar projet en tant que membre de l'équipe.
- Si le AWS CodeStar projet stocke son code source dans CodeCommit les [informations d'identification Git \(informations de connexion\)](#) de l'utilisateur IAM.
- Autorisations requises pour installer Eclipse et l'AWS Toolkit for Eclipse sur votre ordinateur local.

Rubriques

- [Étape 1 : Installer AWS Toolkit for Eclipse](#)
- [Étape 2 : Importer votre projet AWS CodeStar dans Eclipse](#)
- [Étape 3 : Modifier un code de projet AWS CodeStar dans Eclipse](#)

Étape 1 : Installer AWS Toolkit for Eclipse

Le Toolkit for Eclipse est un progiciel que vous pouvez ajouter à Eclipse. Il est installé et géré de la même manière que d'autres packages logiciels dans Eclipse. Le AWS CodeStar kit d'outils est inclus dans le Toolkit for Eclipse.

Pour installer le Toolkit for Eclipse avec le AWS CodeStar module

1. Installez Eclipse sur votre ordinateur local. Les versions prises en charge d'Eclipse incluent Luna, Mars et Neon.
2. Téléchargez et installez le Toolkit for Eclipse. Pour plus d'informations, consultez le [Guide de démarrage AWS Toolkit for Eclipse](#).
3. Dans Eclipse, choisissez Help (Aide), puis Install New Software (Installer un nouveau logiciel).
4. Dans Available Software (Logiciels disponibles), choisissez Add (Ajouter).
5. Dans Add Repository (Ajouter un référentiel), choisissez Archive, accédez à l'emplacement dans lequel vous avez enregistré le fichier .zip, et ouvrez-le. Ne remplissez pas le champ Name (Nom) et choisissez OK.
6. Dans Available Software (Logiciels disponibles), choisissez Select all (Sélectionner tout) pour sélectionner à la fois AWS Core Management Tools et Outils pour développeurs, puis choisissez Next (Suivant).
7. Dans Install Details (Détails de l'installation), choisissez Next (Suivant).
8. Dans Review Licenses (Passer en revue les licences), examinez les contrats de licence. Choisissez I accept the terms of the license agreement (J'accepte les termes du contrat de licence), puis choisissez Finish (Terminer). Redémarrez Eclipse.

Étape 2 : Importer votre projet AWS CodeStar dans Eclipse

Après avoir installé le Toolkit for Eclipse, vous pouvez importer AWS CodeStar des projets et modifier, valider et envoyer du code depuis l'IDE.

 Note

Vous pouvez ajouter plusieurs projets AWS CodeStar à un seul espace de travail dans Eclipse, mais dans ce cas, vous devez mettre à jour vos informations d'identification de projet lorsque vous passez d'un projet à l'un autre.

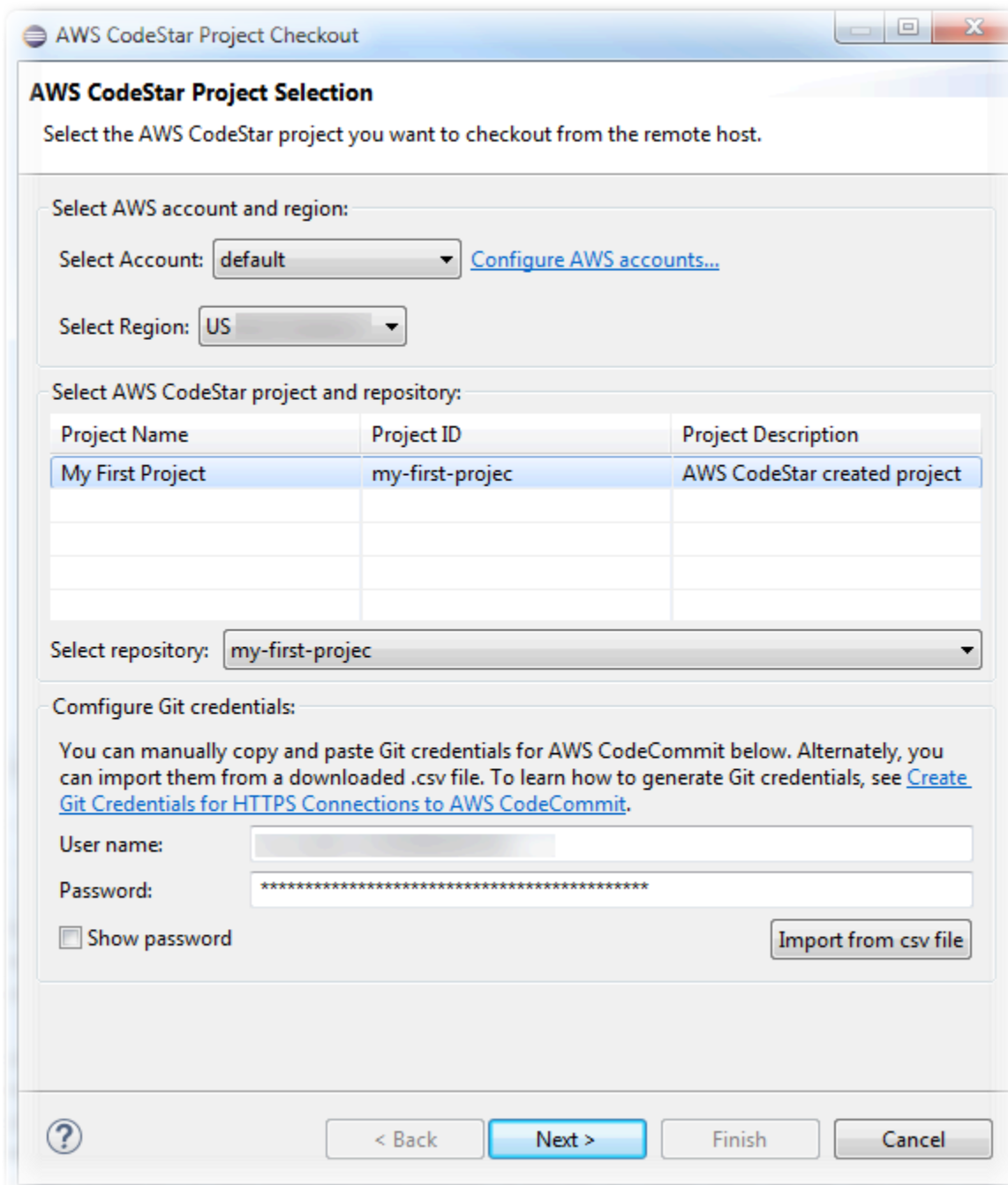
Pour importer un projet AWS CodeStar.

1. Dans le menu AWS, choisissez Importer votre projet AWS CodeStar. Sinon, choisissez Fichier, puis Importer. Dans Sélectionner, développez AWS, puis choisissez Projet AWS CodeStar.

Choisissez Suivant.

2. Dans Sélection AWS CodeStar du projet, choisissez votre AWS profil et la AWS région dans laquelle le AWS CodeStar projet est hébergé. Si aucun AWS profil n'est configuré avec une clé d'accès et une clé secrète sur votre ordinateur, choisissez Configurer les AWS comptes et suivez les instructions.

Dans Sélectionner un AWS CodeStar projet et un référentiel, choisissez votre AWS CodeStar projet. Dans Configurer les informations d'identification Git, entrez les informations de connexion que vous avez générées pour accéder au référentiel du projet. (Si vous ne disposez pas d'informations d'identification Git, consultez [Mise en route](#).) Choisissez Suivant.



3. Toutes les branches du référentiel de projet sont sélectionnées par défaut. Si vous ne souhaitez pas importer une ou plusieurs branches, décochez les cases et choisissez Suivant.
4. Dans Local Destination (Destination locale), choisissez la destination dans laquelle l'assistant d'importation crée le rapport local sur votre ordinateur, puis choisissez Terminer.
5. Dans Project Explorer (Explorateur de projets), développez l'arborescence du projet pour accéder aux fichiers du projet AWS CodeStar.

Étape 3 : Modifier un code de projet AWS CodeStar dans Eclipse

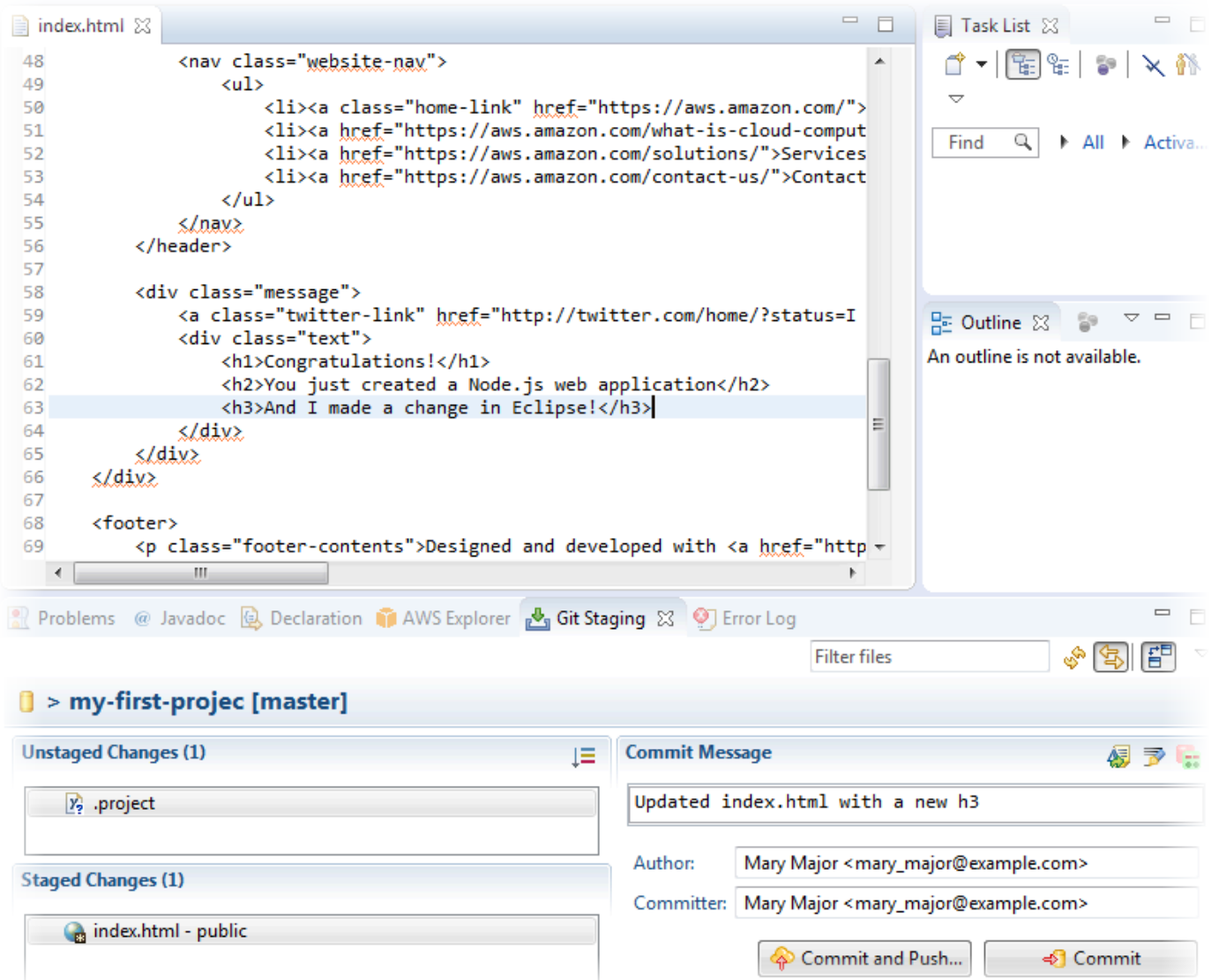
Après avoir importé un projet AWS CodeStar dans un espace de travail Eclipse, vous pouvez modifier le code du projet, enregistrer vos modifications, puis valider et transmettre votre code au référentiel source du projet. Il s'agit de la même procédure que pour n'importe quel référentiel Git utilisant le plug-in EGit pour Eclipse. Pour plus d'informations, consultez le [guide de l'utilisateur EGit](#) sur le site web Eclipse.

Pour modifier le code de projet et effectuez votre première validation du référentiel source pour un projet AWS CodeStar

1. Dans Project Explorer (Explorateur de projets), développez l'arborescence du projet pour accéder aux fichiers du projet AWS CodeStar.
2. Modifiez un ou plusieurs fichiers de code et enregistrez vos modifications.
3. Lorsque vous êtes prêt à valider vos modifications, ouvrez le menu contextuel de ce fichier, choisissez Team (Équipe), puis Commit (Valider).

Vous pouvez ignorer cette étape si la fenêtre Git Staging (Zone intermédiaire Git) est déjà ouverte dans l'affichage de votre projet.

4. Dans Git Staging (Zone intermédiaire Git), organisez vos modifications en déplaçant les fichiers modifiés dans Staged Changes (Modifications intermédiaires). Entrez un message de validation dans Commit Message (Message de validation), puis choisissez Commit and Push (Valider et envoyer).



Pour afficher le déploiement des modifications apportées au code, revenez au tableau de bord de votre projet. Pour plus d'informations, veuillez consulter [Étape 3 : Afficher votre projet](#).

Utilisez Visual Studio avec AWS CodeStar

Vous pouvez utiliser Visual Studio pour modifier le code et développer des logiciels dans un AWS CodeStar projet.

Note

Visual Studio pour Mac ne prend pas en charge le AWS Toolkit et ne peut donc pas être utilisé avec AWS CodeStar.

Les informations de cette section s'appliquent uniquement aux projets AWS CodeStar dont le code source est stocké dans CodeCommit. Si votre AWS CodeStar projet stocke son code source dans GitHub, vous pouvez utiliser un outil tel que l' GitHub extension pour Visual Studio. Pour plus d'informations, consultez la page de [présentation](#) sur le site Web de l' GitHub extension pour Visual Studio et la page [Getting Started with GitHub for Visual Studio](#) sur le GitHub site Web.

Pour utiliser Visual Studio pour modifier le code dans le référentiel source pour un projet AWS CodeStar, vous devez installer une version d'AWS Toolkit for Visual Studio qui prend en charge AWS CodeStar. Vous devez être un membre de l'équipe du projet AWS CodeStar disposant du rôle de propriétaire ou de participant.

Pour utiliser Visual Studio, vous avez également besoin des éléments suivants :

- Utilisateur IAM qui a été ajouté à un AWS CodeStar projet en tant que membre de l'équipe.
- AWS les informations d'identification de votre utilisateur IAM (par exemple, votre clé d'accès et votre clé secrète).
- Les autorisations requises pour installer Visual Studio et AWS Toolkit for Visual Studio sur votre ordinateur local.

Le Toolkit for Visual Studio est un package logiciel que vous pouvez ajouter à Visual Studio. Il est installé et géré de la même manière que les autres packages logiciels de Visual Studio.

Pour installer le Toolkit for Visual Studio avec le AWS CodeStar module et configurer l'accès au référentiel de votre projet

1. Installez Visual Studio sur votre ordinateur local.
2. Téléchargez et installez le Toolkit for Visual Studio et enregistrez le fichier .zip dans un dossier ou un répertoire local. Sur la AWS Toolkit for Visual Studio page Mise en route, entrez ou importez vos AWS informations d'identification, puis choisissez Enregistrer et fermer.
3. Dans Visual Studio, ouvrez Team Explorer. Dans Hosted Service Providers (Fournisseurs de service hébergés), recherchez CodeCommit, puis choisissez Connect.
4. Dans Manage Connections, choisissez Clone. Choisissez le référentiel de votre projet et le dossier dans lequel vous souhaitez cloner le référentiel sur votre ordinateur local, puis choisissez OK.

5. Si vous êtes invité à créer des informations d'identification Git, choisissez Oui. La boîte à outils tente de créer des informations d'identification en votre nom. Enregistrez le fichier d'informations d'identification dans un emplacement sûr. C'est votre seule occasion d'enregistrer ces informations d'identification. Si la boîte à outils ne peut pas créer d'informations d'identification en votre nom ou que vous choisissez Non, vous devez créer et fournir vos propres informations d'identification Git. Pour plus d'informations, consultez [Pour configurer votre ordinateur pour valider les modifications \(utilisateur IAM\)](#) ou suivez les instructions en ligne.

Lorsque vous avez terminé de cloner le projet, vous êtes prêt à modifier votre code dans Visual Studio, puis à valider et à transférer vos modifications dans CodeCommit le référentiel de votre projet.

Modifier les ressources AWS dans un projet AWS CodeStar

Après avoir créé un projet dans AWS CodeStar, vous pouvez modifier l'ensemble de ressources AWS par défaut qu'AWS CodeStar ajoute au projet.

Modifications des ressources prises en charge

Le tableau suivant répertorie les modifications prises en charge apportées aux ressources AWS par défaut dans un projet AWS CodeStar.

Modification	Remarques
Ajouter une étape à AWS CodePipeline.	Consultez Ajouter une étape à AWS CodePipeline .
Modifiez les paramètres de l'environnement d'Elastic Beanstalk.	Consultez Modifier des paramètres de l'environnement AWS Elastic Beanstalk .
Modifiez le code ou les paramètres d'une AWS Lambda fonction, son rôle IAM ou son API dans Amazon API Gateway.	Consultez Modifier une fonction AWS Lambda dans le code source .
Ajouter une ressource à un projet AWS Lambda et développer les autorisations nécessaires pour créer une ressource et y accéder.	Consultez Ajout d'une ressource à un projet .

Modification	Remarques
Ajoutez le transfert de trafic avec CodeDeploy for an AWS Lambda function.	Consultez Déplacer le trafic pour un projet AWS Lambda .
Ajouter une prise en charge AWS X-Ray	Consultez Activer le suivi d'un projet .
Modifiez le fichier buildspec.yml pour votre projet afin d'ajouter une phase de génération de test d'unité exécutée par AWS CodeBuild.	Consultez Étape 7 : Ajouter un test unitaire pour le service web dans le didacticiel Projet sans serveur.
Ajoutez votre propre rôle IAM à votre projet.	Consultez Ajoutez un rôle IAM à un projet .
Modifiez la définition d'un rôle IAM.	Pour les rôles définis dans la pile d'applications. Vous ne pouvez pas modifier les rôles définis dans la chaîne d'outils ou les piles AWS CloudFormation.
Modifiez votre projet Lambda pour ajouter un point de terminaison.	
Modifiez votre projet EC2 pour ajouter un point de terminaison.	
Modifiez votre projet Elastic Beanstalk pour ajouter un point de terminaison.	
Modifiez votre projet pour ajouter une étape Prod et un point de terminaison.	Consultez Ajoutez une étape de prod et un point de terminaison à un projet .
Utiliser en toute sécurité des paramètres SSM dans un projet AWS CodeStar.	Consultez the section called "Utiliser les paramètres SSM en toute sécurité dans un projet AWS CodeStar" .

Les modifications suivantes ne sont pas prises en charge.

- Basculer vers une autre cible de déploiement (par exemple, déployer sur AWS Elastic Beanstalk au lieu d'AWS CodeDeploy).
- Ajouter un nom de point de terminaison web.

- Modifiez le nom du CodeCommit référentiel (pour un AWS CodeStar projet connecté à CodeCommit).
- Pour un AWS CodeStar projet connecté à GitHub, déconnectez le GitHub référentiel, puis reconnectez le référentiel à ce projet, ou connectez tout autre référentiel à ce projet. Vous pouvez utiliser la CodePipeline console (et non la AWS CodeStar console) pour vous déconnecter et vous reconnecter GitHub à l'étape Source d'un pipeline. Toutefois, si vous reconnectez le stage Source à un autre GitHub référentiel, dans le AWS CodeStar tableau de bord du projet, les informations contenues dans les vignettes Repository et Issues peuvent être incorrectes ou obsolètes. La déconnexion du GitHub référentiel ne supprime pas les informations de ce référentiel de l'historique des validations et génère GitHub des vignettes dans le tableau de bord du AWS CodeStar projet. Pour supprimer ces informations, utilisez le GitHub site Web pour désactiver GitHub l'accès au AWS CodeStar projet. Pour révoquer l'accès, sur le GitHub site Web, utilisez la section Applications OAuth autorisées de la page des paramètres du profil de votre GitHub compte.
- Déconnectez le CodeCommit référentiel (pour un AWS CodeStar projet connecté à CodeCommit), puis reconnectez le référentiel à ce projet, ou connectez tout autre référentiel à ce projet.

Ajouter une étape à AWS CodePipeline

Vous pouvez ajouter une nouvelle étape à un pipeline créé par AWS CodeStar dans un projet. Pour plus d'informations, voir [Modifier un pipeline AWS CodePipeline dans](#) le guide de AWS CodePipeline l'utilisateur.

Note

Si la nouvelle étape dépend d'une ressource AWS non créée par AWS CodeStar, il se peut que le pipeline casse. Cela est dû au fait que le rôle IAM AWS CodeStar créé pour n'a AWS CodePipeline peut-être pas accès à ces ressources par défaut.

Pour tenter de donner AWS CodePipeline accès à AWS des ressources qui AWS CodeStar n'ont pas été créées, vous souhaitez peut-être modifier le rôle IAM AWS CodeStar créé. Cela n'est pas pris en charge car AWS CodeStar cela peut supprimer les modifications de votre rôle IAM lorsqu'il effectue des vérifications de mise à jour régulières sur le projet.

Modifier des paramètres de l'environnement AWS Elastic Beanstalk

Vous pouvez modifier les paramètres d'un AWS CodeStar environnement Elastic Beanstalk créé dans un projet. Par exemple, vous souhaitez peut-être modifier l'environnement Elastic

Beanstalk par défaut de votre projet en le faisant passer d'une instance unique AWS CodeStar à un environnement Load Balanced. Pour ce faire, modifiez le fichier `template.yml` dans le référentiel de votre projet. Vous pouvez également avoir besoin de modifier les autorisations pour les rôles de collaborateur de votre projet. Une fois que les changements du modèle ont été transmis en mode push, AWS CodeStar et AWS CloudFormation provisionnent les ressources pour vous.

Pour plus d'informations sur la modification du fichier `template.yml`, consultez [Modifier les ressources de l'application à l'aide du fichier Template.yml](#). Pour plus d'informations sur les environnements Elastic Beanstalk [AWS Elastic Beanstalk, consultez la section Environment Management Console](#) dans le manuel du développeur. AWS Elastic Beanstalk

Modifier une fonction AWS Lambda dans le code source

Vous pouvez modifier le code ou les paramètres d'une fonction Lambda, son rôle IAM ou son API Gateway, AWS CodeStar crée dans un projet. Pour ce faire, nous vous recommandons d'utiliser le modèle d'application AWS sans serveur (AWSSAM) avec le `template.yaml` fichier du CodeCommit référentiel de votre projet. Ce `template.yaml` fichier définit le nom, le gestionnaire, le moteur d'exécution, le rôle IAM et l'API de votre fonction dans API Gateway. Pour plus d'informations, consultez la section [Comment créer des applications sans serveur à l'aide de AWS SAM](#) sur le GitHub site Web.

Activer le suivi d'un projet

AWS X-Ray offre le suivi, que vous pouvez utiliser pour analyser le comportement des performances des applications distribuées (par exemple, les latences dans les temps de réponse). Une fois que vous avez ajouté les trace à votre projet AWS CodeStar, vous pouvez utiliser la console AWS X-Ray pour afficher des vues et des temps de réponse de l'application.

Note

Vous pouvez utiliser ces étapes pour les projets suivants, créés avec les modifications de prise en charge de projet suivantes :

- Tout projet Lambda.
- Pour les projets Amazon EC2 ou Elastic Beanstalk créés après le 3 août 2018AWS CodeStar, provisionnez un fichier dans le référentiel de projets. `/template.yml`

Chaque AWS CodeStar modèle inclut un AWS CloudFormation fichier qui modélise les dépendances AWS d'exécution de votre application, telles que les tables de base de données et les fonctions Lambda. Ce fichier est stocké dans votre référentiel source dans le fichier `/template.yml`.

Vous pouvez modifier ce fichier pour ajouter les traces en ajoutant la ressource AWS X-Ray à la section `Resources`. Vous modifiez ensuite les autorisations IAM pour votre projet de manière à autoriser AWS CloudFormation à créer la ressource. Pour plus d'informations sur les éléments du modèle et le formatage, consultez la section [Référence AWS des types de ressources](#).

Voici les étapes générales à suivre pour personnaliser votre modèle.

1. [Étape 1 : modifier le rôle de travail dans IAM pour le suivi](#)
2. [Étape 2 : modifier le fichier `template.yml` pour le suivi](#)
3. [Étape 3 : valider et transférer votre modification de modèle pour le suivi](#)
4. [Étape 4 : surveiller la mise à jour de la pile AWS CloudFormation pour le suivi](#)

Étape 1 : modifier le rôle de travail dans IAM pour le suivi

Vous devez être connecté en tant qu'administrateur pour effectuer les étapes 1 et 4. Cette étape montre un exemple de modification des autorisations pour un projet Lambda.

Note

Vous pouvez ignorer cette étape si votre projet était configuré avec une stratégie de limite de permissions.

Pour les projets créés après le 6 décembre 2018 PDT, configurez AWS CodeStar votre projet avec une politique de limites d'autorisations.

1. Connectez-vous à la AWS CodeStar console AWS Management Console et ouvrez-la à l'adresse <https://console.aws.amazon.com/codestar/>.
2. Créez un projet ou choisissez un projet existant avec un `template.yml` file, puis ouvrez la page Ressources du projet.
3. Sous Ressources du projet, recherchez le rôle IAM créé pour le rôle CodeStarWorker / Lambda dans la liste des ressources. Le nom du rôle respecte le format suivant : `role/CodeStarWorker-Project_name-lambda-Function_name`. Choisissez l'ARN de ce rôle.

- Le rôle ouvre la console IAM. Sélectionnez Attach Policies (Attacher des politiques). Recherchez la stratégie AWSXrayWriteOnlyAccess, cochez la case en regard, puis choisissez Attach Policy (Attacher une stratégie).

Étape 2 : modifier le fichier template.yml pour le suivi

- Ouvrez la AWS CodeStar console à l'[adresse https://console.aws.amazon.com/codestar/](https://console.aws.amazon.com/codestar/).
- Choisissez votre projet sans serveur, puis ouvrez la page Code. Dans le niveau supérieur de votre référentiel, localisez et modifiez le fichier template.yml. Sous Resources, collez la ressource dans la section Properties.

Tracing: Active

Cet exemple présente un modèle modifié :

```
Resources:
  GetHelloWorld:
    Type: AWS::Serverless::Function
    Properties:
      Handler: index.get
      Runtime: nodejs1.3
      Tracing: Active # Enable X-Ray tracing for the function
    Role:
      Fn::ImportValue:
        !Join ['-', [!Ref 'ProjectId', !Ref 'AWS::Region', 'LambdaTrustRole']]
    Events:
      GetEvent:
        Type: Api
        Properties:
          Path: /
          Method: get
```

Étape 3 : valider et transférer votre modification de modèle pour le suivi

- Validez et transférez les modifications dans le fichier template.yml.

Note

Votre pipeline est démarré. Si vous validez les modifications avant de mettre à jour les autorisations IAM, votre pipeline démarre, la mise à jour de la pile AWS CloudFormation rencontre des erreurs et la mise à jour de la pile est annulée. Si cela se produit, corrigez les autorisations, puis redémarrez votre pipeline.

Étape 4 : surveiller la mise à jour de la pile AWS CloudFormation pour le suivi

1. La mise à jour de la pile AWS CloudFormation démarre lorsque le pipeline de votre projet commence l'étape de déploiement. Pour voir l'état de la mise à jour de la pile, sur votre tableau de bord AWS CodeStar, choisissez l'étape AWS CloudFormation dans votre pipeline.

Si la mise à jour de la pile dans AWS CloudFormation renvoie des erreurs, consultez les instructions de dépannage dans [AWS CloudFormation : Création de la pile annulée en raison d'autorisations manquantes](#). Si des autorisations manquent dans le rôle de travail, modifiez la stratégie attachée au rôle de travail Lambda de votre projet. Consultez [Étape 1 : modifier le rôle de travail dans IAM pour le suivi](#).

2. Utilisez le tableau de bord pour afficher la réussite de l'exécution de votre pipeline. Le suivi est maintenant activé sur votre application.
3. Vérifiez que le suivi est activé en affichant les détails de votre fonction dans la console Lambda.
4. Choisissez le point de terminaison de l'application pour votre projet. Cette interaction avec votre application est suivie. Vous pouvez afficher les informations de suivi sur la console AWS X-Ray.

Trace list					
ID	Age	Method	Response	Response time	URL
...315e2d41	4.7 min		200	270 ms	
...88c0c37c	12.8 sec		200	23.0 ms	

Ajout d'une ressource à un projet

Chaque AWS CodeStar modèle pour tous les projets est fourni avec un AWS CloudFormation fichier qui modélise les dépendances AWS d'exécution de votre application, telles que les tables de base de données et les fonctions Lambda. Ce fichier est stocké dans votre référentiel source dans le fichier `/template.yml`.

Note

Vous pouvez utiliser ces étapes pour les projets suivants, créés avec les modifications de prise en charge de projet suivantes :

- Tout projet Lambda.

- Pour les projets Amazon EC2 ou Elastic Beanstalk créés après le 3 août 2018 AWS CodeStar, provisionnez un fichier dans le référentiel de projets. `/template.yml`

Vous pouvez modifier ce fichier en ajoutant des ressources AWS CloudFormation à la section `Resources`. La modification du fichier `template.yml` permet à AWS CodeStar et AWS CloudFormation d'ajouter la nouvelle ressource à votre projet. Certaines ressources nécessitent que vous ajoutiez d'autres autorisations à la politique relative au rôle de CloudFormation travailleur de votre projet. Pour plus d'informations sur les éléments du modèle et le formatage, consultez la section [Référence AWS des types de ressources](#).

Une fois que vous avez déterminé les ressources que vous devez ajouter à votre projet, voici la procédure générale à suivre pour personnaliser un modèle. Pour obtenir la liste des AWS CloudFormation ressources et leurs propriétés requises, consultez la section [Référence AWS des types de ressources](#).

1. [Étape 1 : Modifier le rôle du CloudFormation travailleur dans IAM](#) (si nécessaire)
2. [Étape 2 : modifier le fichier `template.yml`](#)
3. [Étape 3 : valider et transférer votre modification de modèle](#)
4. [Étape 4 : surveiller la mise à jour de la pile AWS CloudFormation](#)
5. [Étape 5 : ajouter des autorisations de ressources avec une stratégie en ligne](#)

Suivez les étapes décrites dans cette section pour modifier votre modèle de AWS CodeStar projet afin d'ajouter une ressource, puis d'étendre les autorisations du rôle de CloudFormation travailleur du projet dans IAM. Dans cet exemple, la [AWS::SQS::Queue](#) ressource est ajoutée au `template.yml` fichier. La modification déclenche une réponse automatique AWS CloudFormation qui ajoute une file d'attente Amazon Simple Queue Service à votre projet.

Étape 1 : Modifier le rôle du CloudFormation travailleur dans IAM


Vous devez être connecté en tant qu'administrateur pour effectuer les étapes 1 et 5.

Note

Vous pouvez ignorer cette étape si votre projet était configuré avec une stratégie de limite de permissions.

Pour les projets créés après le 6 décembre 2018 PDT, configurez AWS CodeStar votre projet avec une politique de limites d'autorisations.

1. Connectez-vous à la AWS CodeStar console AWS Management Console et ouvrez-la à l'adresse <https://console.aws.amazon.com/codestar/>.
2. Créez un projet ou choisissez un projet existant avec un `template.yml` file, puis ouvrez la page Ressources du projet.
3. Sous Ressources du projet, recherchez le rôle IAM créé pour le AWS CloudFormation rôle CodeStarWorker/dans la liste des ressources. Le nom du rôle respecte le format suivant : `role/CodeStarWorker-Project_name-CloudFormation`.
4. Le rôle ouvre la console IAM. Dans l'onglet Autorisations dans Stratégies en ligne, développez la ligne de votre stratégie de rôle de service, puis choisissez Modifier la stratégie.
5. Choisissez l'onglet JSON pour modifier la stratégie.

 Note

La stratégie attachée au rôle de travail est `CodeStarWorkerCloudFormationRolePolicy`.

6. Dans le champ JSON, ajoutez la déclaration de stratégie suivante dans l'élément Statement.

```
{
  "Action": [
    "sqs:CreateQueue",
    "sqs>DeleteQueue",
    "sqs:GetQueueAttributes",
    "sqs:SetQueueAttributes",
    "sqs:ListQueues",
    "sqs:GetQueueUrl"
  ],
  "Resource": [
    "*"
  ],
  "Effect": "Allow"
}
```

7. Choisissez Examiner une stratégie afin de vous assurer que la stratégie ne contient aucune erreur, puis choisissez Enregistrer les modifications.

Étape 2 : modifier le fichier template.yml

1. Ouvrez la AWS CodeStar console à l'[adresse https://console.aws.amazon.com/codestar/](https://console.aws.amazon.com/codestar/).
2. Choisissez votre projet sans serveur, puis ouvrez la page Code. Au niveau supérieur de votre référentiel, prenez note de l'emplacement de `template.yml`.
3. Utilisez un IDE, la console ou la ligne de commande dans votre référentiel local pour modifier le fichier `template.yml` dans votre référentiel. Collez la ressource dans la section Resources. Dans cet exemple, lorsque le texte suivant est copié, il ajoute la section Resources.

```
Resources:
  TestQueue:
    Type: AWS::SQS::Queue
```

Cet exemple présente un modèle modifié :

```
Resources:
  HelloWorld:
    Type: AWS::Serverless::Function
    Properties:
      Handler: index.handler
      Runtime: python3.6
      Role:
        Fn::ImportValue:
          !Join ['-', [!Ref 'ProjectId', !Ref 'AWS::Region', 'LambdaTrustRole']]
    Events:
      GetEvent:
        Type: Api
        Properties:
          Path: /
          Method: get
      PostEvent:
        Type: Api
        Properties:
          Path: /
          Method: post
  TestQueue:
    Type: AWS::SQS::Queue
```

Étape 3 : valider et transférer votre modification de modèle

- Validez et transférez les modifications dans le fichier `template.yml` que vous avez enregistré à l'étape 2.

Note

Votre pipeline est démarré. Si vous validez les modifications avant de mettre à jour les autorisations IAM, votre pipeline démarre et la mise à jour de la pile AWS

CloudFormation rencontre des erreurs, ce qui entraîne l'annulation de la mise à jour de la pile. Si cela se produit, corrigez les autorisations, puis redémarrez votre pipeline.

Étape 4 : surveiller la mise à jour de la pile AWS CloudFormation

1. La mise à jour de la pile AWS CloudFormation démarre lorsque le pipeline de votre projet commence l'étape Déployer. Vous pouvez choisir l'étape AWS CloudFormation dans votre pipeline dans votre tableau de bord AWS CodeStar pour voir la mise à jour de la pile.

Résolution de problèmes

La mise à jour de la pile échoue si les autorisations des ressources requises sont manquantes. Affichez l'état de défaillance dans le tableau de bord AWS CodeStar pour le pipeline de votre projet.

Choisissez le CloudFormation lien dans la phase de déploiement de votre pipeline pour résoudre le problème de la AWS CloudFormation console. Dans la console, dans la liste Événements, choisissez votre projet pour afficher les détails de création de la pile. Un message présente les détails de l'échec. Dans cet exemple, l'autorisation `sqs:CreateQueue` est manquante.

08:37:11 UTC-0700	UPDATE_ROLLBACK_COMPLETE	AWS::CloudFormation::Stack	awscodestar-dk-sqs-red-lambda	
08:37:11 UTC-0700	DELETE_COMPLETE	AWS::SQS::Queue	TestQueue	
08:37:09 UTC-0700	UPDATE_ROLLBACK_COMPLETE_CLEANUP_IN_PROGRESS	AWS::CloudFormation::Stack	awscodestar-dk-sqs-red-lambda	
08:37:06 UTC-0700	UPDATE_COMPLETE	AWS::Lambda::Function	HelloWorld	
08:37:03 UTC-0700	UPDATE_ROLLBACK_IN_PROGRESS	AWS::CloudFormation::Stack	awscodestar-dk-sqs-red-lambda	The following resource(s) failed to create: [TestQueue]. The following resource(s) failed to update: [HelloWorld].
08:37:02 UTC-0700	UPDATE_FAILED	AWS::Lambda::Function	HelloWorld	Resource update cancelled
08:37:01 UTC-0700	CREATE_FAILED	AWS::SQS::Queue	TestQueue	API: sqs:CreateQueue Access to the resource https://sqs.us-west-2.amazonaws.com/ is denied.
08:37:01 UTC-0700	CREATE_IN_PROGRESS	AWS::SQS::Queue	TestQueue	

Ajoutez les autorisations manquants en modifiant la stratégie attachée au rôle de travail AWS CloudFormation de votre projet. Consultez [Étape 1 : Modifier le rôle du CloudFormation travailleur dans IAM](#).

2. Après une exécution réussie de votre pipeline, les ressources sont créées dans votre pile AWS CloudFormation. Dans la liste Ressources dans AWS CloudFormation, consultez la ressource créée pour votre projet. Dans cet exemple, la TestQueue file d'attente est répertoriée dans la section Ressources.

L'URL de file d'attente est disponible dans AWS CloudFormation. Le format de l'URL de file d'attente est le suivant :

```
https://{REGION_ENDPOINT}/queue.|api-domain|/{YOUR_ACCOUNT_NUMBER}/  
{YOUR_QUEUE_NAME}
```

Pour plus d'informations, consultez [Envoyer un message Amazon SQS](#), [Recevoir un message d'une file d'attente Amazon SQS](#) et [Supprimer un message d'une file d'attente Amazon SQS](#).

Étape 5 : ajouter des autorisations de ressources avec une stratégie en ligne

Accorder aux membres de l'équipe l'accès à votre nouvelle ressource en ajoutant la stratégie en ligne adaptée au rôle de l'utilisateur. Les ressources ne nécessitent pas toutes que vous ajoutiez des autorisations. Pour effectuer les étapes suivantes, vous devez vous être connecté à la console soit en tant qu'utilisateur root, soit en tant qu'utilisateur administrateur du compte, soit en tant qu'utilisateur IAM ou utilisateur fédéré avec la politique AdministratorAccess gérée ou un équivalent.

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 Politiques (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 :

```
{  
  "Action": [  
    "sqs:CreateQueue",  
    "sqs>DeleteQueue",  
    "sqs:GetQueueAttributes",  
    "sqs:SetQueueAttributes",  
    "sqs:ListQueues",  
    "sqs:GetQueueUrl"  
  ],  
  "Resource": [  
    "*"   
  ],  
}
```

```
"Effect": "Allow"
}
```

6. Choisissez 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, consultez [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.

Ajoutez un rôle IAM à un projet

Vous pouvez définir vos propres rôles et stratégies dans la pile d'applications (template.yml) depuis. Pour atténuer les risques d'escalade des privilèges et les actions de destruction, vous devez définir la limite d'autorisations spécifique au projet pour chaque entité IAM que vous créez. Si vous avez un projet Lambda avec plusieurs fonctions, il est recommandé de créer un rôle IAM pour chaque fonction.

Pour ajouter un rôle IAM à votre projet

1. Modifiez le fichier `template.yml` pour votre projet.
2. Dans la section `Resources:`, ajoutez votre ressource IAM, en utilisant le format dans l'exemple suivant :

```
SampleRole:
  Description: Sample Lambda role
  Type: AWS::IAM::Role
  Properties:
    AssumeRolePolicyDocument:
      Statement:
```

```
- Effect: Allow
Principal:
  Service: [lambda.amazonaws.com]
Action: sts:AssumeRole
ManagedPolicyArns:
  - arn:aws:iam::aws:policy/service-role/AWSLambdaBasicExecutionRole
PermissionsBoundary: !Sub 'arn:${AWS::Partition}:iam:${AWS::AccountId}:policy/CodeStar_${ProjectId}_PermissionsBoundary'
```

3. Publiez vos modifications via le pipeline et vérifiez la réussite.

Ajoutez une étape de prod et un point de terminaison à un projet

Utilisez les procédures de cette section pour ajouter une nouvelle étape de production (Prod) à votre pipeline et une étape d'approbation manuelle entre les étapes Déploiement et Prod de votre pipeline. Cela crée une pile de ressources supplémentaires lorsque votre projet de pipeline s'exécute.

Note

Vous pouvez utiliser ces procédures si :

- Pour les projets créés après le 3 août 2018, AWS CodeStar provisionne votre projet Amazon EC2, Elastic Beanstalk ou Lambda avec un fichier dans le référentiel de projets. /`template.yml`
- Pour les projets créés après le 6 décembre 2018 PDT, configurez AWS CodeStar votre projet avec une politique de limites d'autorisations.

Tous les AWS CodeStar projets utilisent un fichier AWS CloudFormation modèle qui modélise les dépendances AWS d'exécution de votre application, telles que les instances Linux et les fonctions Lambda. Ce fichier /`template.yml` est stocké dans votre référentiel source.

Dans le fichier /`template.yml`, utilisez le paramètre `Stage` pour ajouter une pile de ressources pour une nouvelle étape dans le pipeline du projet.

```
Stage:
  Type: String
  Description: The name for a project pipeline stage, such as Staging or Prod, for
  which resources are provisioned and deployed.
```



```
Default: ''
```

Le paramètre Stage est appliqué à toutes les ressources nommées avec l'ID de projet référencé dans la ressource. Par exemple, le nom de rôle suivant est une ressource nommée dans le modèle :

```
RoleName: !Sub 'CodeStar-${ProjectId}-WebApp${Stage}'
```

Prérequis

Utilisez les options du modèle dans la console AWS CodeStar pour créer un projet.

Assurez-vous que votre utilisateur IAM dispose des autorisations suivantes :

- `iam:PassRole` sur le rôle AWS CloudFormation du projet.
- `iam:PassRole` sur le rôle de chaîne d'outils du projet.
- `cloudformation:DescribeStacks`
- `cloudformation:ListChangeSets`

Pour les projets Elastic Beanstalk ou Amazon EC2 uniquement :

- `codedeploy:CreateApplication`
- `codedeploy:CreateDeploymentGroup`
- `codedeploy:GetApplication`
- `codedeploy:GetDeploymentConfig`
- `codedeploy:GetDeploymentGroup`
- `elasticloadbalancing:DescribeTargetGroups`

Rubriques

- [Étape 1 : créer un nouveau groupe de déploiement dans CodeDeploy \(projets Amazon EC2 uniquement\)](#)
- [Étape 2 : ajout d'une nouvelle étape pipeline pour l'étape prod](#)
- [Étape 3 : ajouter une étape d'approbation manuelle](#)
- [Étape 4 : transmission d'une modification et surveillance de la mise à jour de pile AWS CloudFormation](#)

Étape 1 : créer un nouveau groupe de déploiement dans CodeDeploy (projets Amazon EC2 uniquement)

Vous choisissez votre CodeDeploy application, puis vous ajoutez un nouveau groupe de déploiement associé à la nouvelle instance.

Note

Si votre projet est un projet Lambda ou Elastic Beanstalk, vous pouvez ignorer cette étape.

1. Ouvrez la CodeDeploy console à l'[adresse https://console.aws.amazon.com/codedeploy](https://console.aws.amazon.com/codedeploy).
2. Choisissez l' CodeDeploy application qui a été générée pour votre projet lors de sa création dans AWS CodeStar.
3. Sous Deployment groups (Groupes de déploiement), choisissez Create deployment group (Créer un groupe de déploiement).
4. Dans Nom du groupe de déploiement, saisissez **<project-id>-prod-Env**.
5. Dans Rôle de service, choisissez le rôle de travail de chaîne de compilation pour votre projet AWS CodeStar.
6. Sous Type de déploiement, choisissez Sur place.
7. Dans Configuration de l'environnement, choisissez l'onglet Instances Amazon EC2.
8. Dans le groupe de balises, sous Clé, choisissez `aws:cloudformation:stack-name`. Sous Valeur, choisissez `awscodestar-<projectid>-infrastructure-prod` (la pile à créer pour l'GenerateChangeSet action).
9. Dans Paramètres de déploiement, choisissez `CodeDeployDefault.AllAtOnce`.
10. Supprimer Choisir un équilibreur de charge.
11. Choisissez Créer un groupe de déploiement.

Votre deuxième groupe de déploiement est désormais créé.

Étape 2 : ajout d'une nouvelle étape pipeline pour l'étape prod

Ajoutez une étape avec le même ensemble d'actions de déploiement que l'étape Déploiement de votre projet. Par exemple, la nouvelle étape Prod d'un projet Amazon EC2 doit comporter les mêmes actions que l'étape Deploy créée pour le projet.

Pour copier les paramètres et les champs à partir de la phase Déploiement

1. Dans le tableau de bord de votre AWS CodeStar projet, choisissez Détails du pipeline pour ouvrir votre pipeline dans la CodePipeline console.
2. Choisissez Edit (Modifier).
3. Dans la phase Déploiement, choisissez Modifier l'étape.
4. Cliquez sur l'icône d'édition sur l'GenerateChangeSetaction. Notez les valeurs dans les champs suivants. Vous utilisez ces valeurs lorsque vous créez votre nouvelle action.
 - Nom de la pile
 - Modifier le nom du jeu
 - Modèle
 - Configuration de modèle
 - Artefacts d'entrée
5. Développez Advanced (Avancé) et copiez les paramètres de votre projet dans Parameters (Paramètres). Vous collez ces paramètres dans votre nouvelle action. Par exemple, copiez les paramètres qui sont présentés ici au format JSON :

- Projets Lambda :

```
{
  "ProjectId": "MyProject"
}
```

- Projets Amazon EC2 :

```
{
  "ProjectId": "MyProject",
  "InstanceType": "t2.micro",
  "WebAppInstanceProfile": "awscodestar-MyProject-WebAppInstanceProfile-EXAMPLEY5VSFS",
  "ImageId": "ami-EXAMPLE1",
  "KeyPairName": "my-keypair",
  "SubnetId": "subnet-EXAMPLE",
  "VpcId": "vpc-EXAMPLE1"
}
```

- Projets d'Elastic Beanstalk :

```
{
  "ProjectId": "MyProject",
  "InstanceType": "t2.micro",
  "KeyPairName": "my-keypair",
  "SubnetId": "subnet-EXAMPLE",
  "VpcId": "vpc-EXAMPLE",
  "SolutionStackName": "64bit Amazon Linux 2018.03 v3.0.5 running Tomcat 8 Java
8",
  "EBTrustRole": "CodeStarWorker-myproject-EBService",
  "EBInstanceProfile": "awscodestar-myproject-EBInstanceProfile-11111EXAMPLE"
}
```

6. Dans le panneau de modification d'étape, choisissez Annuler.

Pour créer une `GenerateChangeSet` action dans votre nouvelle phase de production


Note

Après avoir ajouté la nouvelle action, si vous êtes encore en mode Édition et que vous rouvrez la nouvelle action pour la modifier, certains champs peuvent ne pas s'afficher. Le message suivant peut aussi s'afficher : `Stack stack-name does not exist`. Cette erreur ne vous empêche pas d'enregistrer le pipeline. Cependant, pour restaurer les champs manquants, vous devez supprimer la nouvelle action et l'ajouter à nouveau. Une fois que vous avez enregistré et exécuté le pipeline, la pile est reconnue et l'erreur ne s'affiche plus.

1. Si votre pipeline n'est pas déjà affiché, dans le tableau de bord de votre AWS CodeStar projet, choisissez Détails du pipeline pour ouvrir votre pipeline dans la console.
2. Choisissez Edit (Modifier).
3. Au bas du diagramme, choisissez + Ajouter une étape.
4. Saisissez un nom d'étape, (par exemple, **Prod**), puis choisissez + Ajout de groupe d'action.
5. Dans Nom d'action, saisissez un nom pour le pipeline (par exemple, **GenerateChangeSet**).
6. Dans Action provider, sélectionnez AWS CloudFormation.
7. Dans Mode d'action, choisissez Créer ou remplacer un jeu de modifications.

8. Dans Nom de pile, saisissez un nouveau nom pour la pile AWS CloudFormation qui doit être créée par cette action. Commencez par un nom qui est identique à la pile Déploiement, puis ajoutez **-prod** :

- Projets Lambda : `awscodestar-<project_name>-lambda-prod`
- Projets Amazon EC2 et Elastic Beanstalk : `awscodestar-<project_name>-infrastructure-prod`

 Note

Le nom de la pile doit commencer exactement par **awscodestar-<project_name>-**, sinon la création de la pile échoue.

9. Dans Change set name (Modifier le nom du jeu), saisissez le même nom de jeu que celui fourni dans l'étape Déploiement existante (par exemple, **pipeline-changeset**).
10. Dans la section Artefacts d'entrée, choisissez l'artefact de génération.
11. Dans Modèle, saisissez le même nom de modèle de modification que celui fourni dans l'étape Déploiement existante (par exemple, **<project-ID>-BuildArtifact::template.yml**).
12. Dans Template configuration (Configuration du modèle), saisissez le même nom de fichier de configuration de modèle que celui fourni dans l'étape de déploiement (par exemple, **<project-ID>-BuildArtifact::template-configuration.json**).
13. Dans Capacités, choisissez `CAPABILITY_NAMED_IAM`.
14. Dans Nom de rôle, choisissez le nom du rôle de travail du AWS CloudFormation de votre projet.
15. Développez Advanced (Avancé) et copiez les paramètres de votre projet dans Parameters (Paramètres). Incluez le Stage paramètre, présenté ici au format JSON, pour un projet Amazon EC2 :

```
{
  "ProjectId": "MyProject",
  "InstanceType": "t2.micro",
  "WebAppInstanceProfile": "awscodestar-MyProject-WebAppInstanceProfile-EXAMPLEY5VSFS",
  "ImageId": "ami-EXAMPLE1",
  "KeyPairName": "my-keypair",
  "SubnetId": "subnet-EXAMPLE",
  "VpcId": "vpc-EXAMPLE1",
```

```
"Stage": "Prod"  
}
```

Note

Assurez-vous de coller tous les paramètres pour le projet et pas seulement les nouveaux paramètres ou les paramètres que vous souhaitez modifier.

16. Choisissez Save (Enregistrer).
17. Dans le volet AWS CodePipeline, choisissez Enregistrer les modifications du pipeline, puis Enregistrer la modification.

Note


Un message peut s'afficher pour vous informer de la suppression et de l'ajout de ressources de détection de modifications. Confirmez réception du message et passez à l'étape suivante de ce didacticiel.

Affichez votre pipeline mis à jour.

Pour créer une ExecuteChangeSet action dans votre nouvelle phase de production

1. Si vous ne consultez pas encore votre pipeline, depuis le tableau de bord de votre AWS CodeStar projet, choisissez Détails du pipeline pour ouvrir votre pipeline dans la console.
2. Choisissez Edit (Modifier).
3. Dans votre nouvelle phase de production, après la nouvelle GenerateChangeSetaction, choisissez + Ajouter un groupe d'actions.
4. Dans Nom d'action, saisissez un nom pour le pipeline (par exemple, **ExecuteChangeSet**).
5. Dans Action provider, sélectionnez AWS CloudFormation.
6. Dans Action mode (Mode d'action), choisissez Execute a change set (Exécuter un jeu de modifications).
7. Dans Nom de la pile, entrez le nouveau nom de la AWS CloudFormation pile que vous avez saisie dans l' GenerateChangeSet action (par exemple, **awscodestar-<project-ID>-infrastructure-prod**).

8. Dans Nom du jeu de modifications, entrez le même nom d'ensemble de modifications que celui utilisé lors de la phase de déploiement (par exemple, **pipeline-changeset**).
9. Sélectionnez Exécuté.
10. Dans le volet AWS CodePipeline, choisissez Enregistrer les modifications du pipeline, puis Enregistrer la modification.

 Note

Un message peut s'afficher pour vous informer de la suppression et de l'ajout de ressources de détection de modifications. Confirmez réception du message et passez à l'étape suivante de ce didacticiel.

Affichez votre pipeline mis à jour.

Pour créer une action de CodeDeploy déploiement dans votre nouvelle phase de production (projets Amazon EC2 uniquement)

1. Une fois les nouvelles actions dans votre étape Prod, choisissez + Action.
2. Dans Nom d'action, saisissez un nom pour le pipeline (par exemple, **Deploy**).
3. Dans Action provider, sélectionnez AWS CodeDeploy.
4. Dans Nom de l'application, choisissez le nom de l' CodeDeployapplication pour votre projet.
5. Dans Groupe de déploiement, choisissez le nom du nouveau groupe de déploiement CodeDeploy que vous avez créé à l'étape 2.
6. Dans Artefacts d'entrée, choisissez le même artefact de génération utilisé dans l'étape existante.
7. Sélectionnez Exécuté.
8. Dans le volet AWS CodePipeline, choisissez Enregistrer les modifications du pipeline, puis Enregistrer la modification. Affichez votre pipeline mis à jour.

Étape 3 : ajouter une étape d'approbation manuelle

La bonne pratique consiste à ajouter une étape d'approbation manuelle avant votre nouvelle étape de production.

1. Dans le coin supérieur gauche, choisissez Modifier.

2. Dans votre schéma de pipeline, entre les étapes de Déploiement et Prod, choisissez + Ajouter une étape.
3. Dans Modifier l'étape, saisissez un nom d'étape (par exemple, **Approval**), puis choisissez + Ajouter groupe d'action.
4. Dans Nom d'action, saisissez un nom pour le pipeline (par exemple, **Approval**).
5. Dans Approval type, choisissez Manual approval.
6. (Facultatif) Sous Configuration, dans SNS Topic ARN, choisissez la rubrique SNS que vous avez créée et à laquelle vous vous êtes abonnés.
7. Sélectionnez Ajouter une action.
8. Dans le volet AWS CodePipeline, choisissez Enregistrer les modifications du pipeline, puis Enregistrer la modification. Affichez votre pipeline mis à jour.
9. Pour soumettre vos modifications et lancer la génération d'un pipeline, choisissez Changement de version, puis Publication.

Étape 4 : transmission d'une modification et surveillance de la mise à jour de pile AWS CloudFormation

1. Pendant que votre pipeline est en cours d'exécution, vous pouvez suivre les étapes décrites ici pour suivre la création de la pile et du point de terminaison pour votre nouvelle étape.
2. Lorsque le pipeline lance l'étape de déploiement, la mise à jour de la pile AWS CloudFormation démarre. Vous pouvez choisir l'étape AWS CloudFormation dans votre pipeline de votre tableau de bord AWS CodeStar pour voir la notification de la mise à jour de la pile. Pour afficher les détails de création de la pile, choisissez votre projet dans la liste Événements de la console.
3. Une fois votre pipeline terminé, les ressources sont créées dans votre pile AWS CloudFormation. Choisissez l'infrastructure de pile pour votre projet dans la console AWS CloudFormation. Les noms de pile suivent ce format :
 - Projets Lambda : `awscodestar-<project_name>-lambda-prod`
 - Projets Amazon EC2 et Elastic Beanstalk : `awscodestar-<project_name>-infrastructure-prod`

Dans la liste Ressources dans la console AWS CloudFormation, consultez la ressource créée pour votre projet. Dans cet exemple, la nouvelle instance Amazon EC2 apparaît dans la section Ressources.

4. Accédez au point de terminaison de votre étape de production :
 - Pour un projet Elastic Beanstalk, ouvrez la nouvelle pile AWS CloudFormation dans la console et développez Resources. Choisissez l'application Elastic Beanstalk. Le lien s'ouvre dans la console Elastic Beanstalk. Choisissez Environnements. Choisissez l'URL dans URL pour ouvrir le point de terminaison dans un navigateur.
 - Pour un projet Lambda, ouvrez la nouvelle pile dans la AWS CloudFormation console et développez Resources. Choisissez la ressource API Gateway. Le lien s'ouvre dans la console API Gateway. Choisissez Stages (Étapes). Choisissez l'URL dans Invoke URL (Invoquer l'URL) pour ouvrir le point de terminaison dans un navigateur.
 - Pour un projet Amazon EC2, choisissez la nouvelle instance Amazon EC2 dans la liste des ressources de votre projet dans la console. AWS CodeStar Le lien s'ouvre sur la page Instance de la console Amazon EC2. Choisissez l'onglet Description, copiez l'URL dans DNS public (IPv4), puis ouvrez l'URL dans un navigateur.
5. Vérifiez que votre modification est déployée.

Utiliser les paramètres SSM en toute sécurité dans un projet AWS CodeStar

De nombreux clients stockent des secrets, tels que des informations d'identification, dans [les paramètres du magasin de paramètres de Systems Manager](#). Vous pouvez désormais utiliser ces paramètres en toute sécurité dans un AWS CodeStar projet. Par exemple, vous souhaitez peut-être utiliser les paramètres SSM dans vos spécifications de compilation pour CodeBuild ou lors de la définition des ressources d'application dans votre pile de chaînes d'outils (template.yml).

Pour utiliser les paramètres SSM dans un CodeStar projet AWS, vous devez baliser manuellement les paramètres avec l'ARN du CodeStar projet AWS. Vous devez également fournir les autorisations appropriées au rôle de travailleur de la CodeStar chaîne d'outils AWS pour accéder aux paramètres que vous avez balisés.

Avant de commencer

- [Créez un nouveau](#) paramètre ou identifiez un paramètre existant de Systems Manager contenant les informations auxquelles vous souhaitez accéder.
- Identifiez le CodeStar projet AWS que vous souhaitez utiliser ou [créez un nouveau projet](#).
- Notez l'ARN du CodeStar projet. Il se présente comme suit : `arn:aws:codestar:region-id:account-id:project/project-id`.

Marquer un paramètre avec l'ARN CodeStar du projet AWS

Pour obtenir des instructions étape par étape, consultez [Balisage des paramètres Systems Manager](#).

1. Dans Clé, entrez `awscodestar:projectArn`.
2. Dans Valeur, entrez l'ARN du projet à partir de CodeStar :`arn:aws:codestar:region-id:account-id:project/project-id`.
3. Choisissez Enregistrer.

Maintenant, vous pouvez référencer le paramètre SSM dans votre fichier `template.yml`. Si vous souhaitez l'utiliser avec un rôle de travail de chaîne d'outils, vous devez accorder des autorisations supplémentaires.

Accordez des autorisations pour utiliser des paramètres balisés dans votre chaîne d'outils de CodeStar projet AWS

Note

Ces étapes ne s'appliquent qu'aux projets créés après le 6 décembre 2018 PDT.

1. Ouvrez le tableau de bord CodeStar du projet AWS correspondant au projet que vous souhaitez utiliser.
2. Cliquez sur Projet pour afficher la liste des ressources créées et recherchez le rôle de travail de chaîne d'outils. Il s'agit d'une ressource IAM avec un nom au format : `role/CodeStarWorker-project-id-ToolChain`.
3. Cliquez sur l'ARN pour l'ouvrir dans la console IAM.
4. Localisez-le ToolChainWorkerPolicy et agrandissez-le, si nécessaire.
5. Cliquez sur Modifier la stratégie.
6. Sous Action:, ajoutez la ligne suivante :

```
ssm:GetParameter*
```

7. Cliquez sur Examiner une stratégie, puis sur Enregistrer les modifications.

Pour les projets créés avant le 6 décembre 2018 PDT, vous devrez ajouter les autorisations suivantes aux rôles des travailleurs pour chaque service.

```
{
  "Action": [
    "ssm:GetParameter*"
  ],
  "Resource": "*",
  "Effect": "Allow",
  "Condition": {
    "StringEquals": {
      "ssm:ResourceTag/awscodestar:projectArn": "arn:aws:codestar:region-
id:account-id:project/project-id"
    }
  }
}
```

Déplacer le trafic pour un projet AWS Lambda

AWS CodeDeploy prend en charge les déploiements de versions de fonctions pour les fonctions AWS Lambda dans vos projets sans serveur AWS CodeStar. Un déploiement AWS Lambda déplace le trafic entrant d'une fonction Lambda existante vers une version de fonction Lambda mise à jour. Vous pouvez tester une fonction Lambda mise à jour en déployant une version distincte, puis en restaurant le déploiement à la première version, le cas échéant.

Suivez les étapes décrites dans cette section pour modifier votre modèle de AWS CodeStar projet et mettre à jour les autorisations IAM de vos CodeStarWorker rôles. Cette tâche lance une réponse automatique dans AWS CloudFormation qui crée des fonctions AWS Lambda disposant d'un alias, puis demande à AWS CodeDeploy de rediriger le trafic vers un environnement mis à jour.

Note

Effectuez ces étapes uniquement si vous avez créé votre CodeStar projet AWS avant le 12 décembre 2018.

AWS CodeDeploy possède trois options de déploiement qui vous permettent de déplacer le trafic vers des versions de votre fonction AWS Lambda dans votre application :

- Canary : le trafic est déplacé en deux incréments. Vous pouvez choisir parmi les options de contrôle de validité prédéfinies qui définissent le pourcentage de trafic déplacé vers la version mise

à jour de votre fonction Lambda dans le premier incrément, et l'intervalle en minutes avant que le trafic restant soit déplacé dans le second incrément.

- **Linéaire** : le trafic est déplacé en incréments égaux, avec un nombre de minutes égal entre chaque incrément. Vous pouvez choisir parmi les options linéaires prédéfinies qui définissent le pourcentage de trafic déplacé pour chaque incrément et le nombre de minutes entre chaque incrément. Le trafic est déplacé en incréments égaux, avec un nombre égal de minutes entre chaque incrément. Vous pouvez choisir parmi les options linéaires prédéfinies qui définissent le pourcentage de trafic déplacé pour chaque incrément et le nombre de minutes entre chaque incrément.
- **R II-at-once** : Tout le trafic est transféré de la fonction Lambda d'origine à la version mise à jour de la fonction Lambda en une fois.

Type de préférence de déploiement

Canary10Percent30Minutes

Canary10Percent5Minutes

Canary10Percent10Minutes

Canary10Percent15Minutes

Linéaire 10 10 minutes PercentEvery

Linéaire 10 1 minute PercentEvery

Linéaire 10 2 minutes PercentEvery

Linéaire 10 3 minutes PercentEvery

AllAtOnce

Pour plus d'informations sur AWS CodeDeploy les déploiements sur une plate-forme de AWS Lambda calcul, consultez la section [Déploiements sur une plate-forme de calcul AWS Lambda](#).

Pour plus d'informations sur AWS SAM, consultez la section [AWSServerless Application Model \(AWSSAM\)](#) on GitHub.

Prérequis :

Lorsque vous créez un projet sans serveur, sélectionnez n'importe quel modèle avec la plateforme de calcul Lambda. Vous devez être connecté en tant qu'administrateur pour effectuer les étapes 4 à 6.

Étape 1 : modifier le modèle SAM pour ajouter les paramètres de déploiement de versions AWS Lambda

1. Ouvrez la AWS CodeStar console à l'[adresse https://console.aws.amazon.com/codestar/](https://console.aws.amazon.com/codestar/).
2. Créez un projet ou choisissez un projet existant avec un fichier `template.yml`, puis ouvrez la page Code. Au niveau supérieur de votre référentiel, notez l'emplacement du modèle SAM nommée `template.yml` à modifier.
3. Ouvrez le fichier `template.yml` dans votre IDE ou référentiel local. Copiez le texte suivant pour ajouter une section `Globals` au fichier. L'exemple de texte dans ce didacticiel choisit l'option `Canary10Percent5Minutes`.

```
Globals:
  Function:
    AutoPublishAlias: live
    DeploymentPreference:
      Enabled: true
      Type: Canary10Percent5Minutes
```

Cet exemple montre un modèle modifié après l'ajout de la section `Globals` :

```
AWSTemplateFormatVersion: 2010-09-09
Transform:
- AWS::Serverless-2016-10-31
- AWS::CodeStar

Parameters:
  ProjectId:
    Type: String
    Description: CodeStar projectId used to associate new resources to team members

Globals:
  Function:
    AutoPublishAlias: live
    DeploymentPreference:
      Enabled: true
      Type: Canary10Percent5Minutes

Resources:
  HelloWorld:
    Type: AWS::Serverless::Function
    Properties:
      Handler: index.handler
      Runtime: python3.6
      Role:
        Fn::ImportValue:
          !Join ['-', [!Ref 'ProjectId', !Ref 'AWS::Region', 'LambdaTrustRole']]
    Events:
```

Pour plus d'informations, consultez le guide de référence [Section Globales](#) pour les modèles SAM.

Étape 2 : modifier le rôle AWS CloudFormation pour ajouter des autorisations

1. Connectez-vous à la AWS CodeStar console AWS Management Console et ouvrez-la à l'adresse <https://console.aws.amazon.com/codestar/>.

Note

Vous devez vous connecter à l'AWS Management Console aide des informations d'identification associées à l'utilisateur IAM que vous avez créé ou dans [Configuration AWS CodeStar](#) lequel vous vous êtes identifié. Cet utilisateur doit disposer de la stratégie gérée AWS nommée **AWSCodeStarFullAccess** attachée.

2. Choisissez votre projet sans serveur existant, puis ouvrez la page Ressources du projet.
3. Sous Ressources, choisissez le rôle IAM créé pour le AWS CloudFormation rôle CodeStarWorker/. Le rôle ouvre la console IAM.
4. Dans l'onglet Autorisations dans Stratégies en ligne, sur la rangée de votre stratégie de rôle de service, choisissez Modifier la stratégie. Choisissez l'onglet JSON pour modifier la stratégie au format JSON.

Note

Votre rôle de service est nommé CodeStarWorkerCloudFormationRolePolicy.

5. Dans le champ JSON, ajoutez les déclarations de stratégie suivantes au sein de l'élément Statement. Remplacez les espaces réservés *region* et *id* par votre région et l'identifiant de votre compte.

```
{
  "Action": [
    "s3:GetObject",
    "s3:GetObjectVersion",
    "s3:GetBucketVersioning"
  ],
  "Resource": "*",
```

```
"Effect": "Allow"
},
{
  "Action": [
    "s3:PutObject"
  ],
  "Resource": [
    "arn:aws:s3:::codepipeline*"
  ],
  "Effect": "Allow"
},
{
  "Action": [
    "lambda:*"
  ],
  "Resource": [
    "arn:aws:lambda:region:id:function:*"
  ],
  "Effect": "Allow"
},
{
  "Action": [
    "apigateway:*"
  ],
  "Resource": [
    "arn:aws:apigateway:region::*"
  ],
  "Effect": "Allow"
},
{
  "Action": [
    "iam:GetRole",
    "iam:CreateRole",
    "iam>DeleteRole",
    "iam:PutRolePolicy"
  ],
  "Resource": [
    "arn:aws:iam::id:role/*"
  ],
  "Effect": "Allow"
},
{
  "Action": [
    "iam:AttachRolePolicy",
```

```
    "iam:DeleteRolePolicy",
    "iam:DetachRolePolicy"
  ],
  "Resource": [
    "arn:aws:iam::id:role/*"
  ],
  "Effect": "Allow"
},
{
  "Action": [
    "iam:PassRole"
  ],
  "Resource": [
    "*"
  ],
  "Effect": "Allow"
},
{
  "Action": [
    "codedeploy:CreateApplication",
    "codedeploy>DeleteApplication",
    "codedeploy:RegisterApplicationRevision"
  ],
  "Resource": [
    "arn:aws:codedeploy:region:id:application:*"
  ],
  "Effect": "Allow"
},
{
  "Action": [
    "codedeploy>CreateDeploymentGroup",
    "codedeploy>CreateDeployment",
    "codedeploy>DeleteDeploymentGroup",
    "codedeploy:GetDeployment"
  ],
  "Resource": [
    "arn:aws:codedeploy:region:id:deploymentgroup:*"
  ],
  "Effect": "Allow"
},
{
  "Action": [
    "codedeploy:GetDeploymentConfig"
  ],
```



```
"Resource": [  
  "arn:aws:codedeploy:region:id:deploymentconfig:*"  
],  
"Effect": "Allow"  
}
```

6. Choisissez Examiner une stratégie afin de vérifier que la stratégie ne contient aucune erreur. Si la stratégie ne contient pas d'erreur, choisissez Enregistrer les modifications.

Étape 3 : valider et transférer votre modification de modèle pour démarrer le déplacement de version AWS Lambda

1. Validez et transférez les modifications dans le fichier `template.yml` que vous avez enregistré à l'étape 1.

Note

Votre pipeline est démarré. Si vous validez les modifications avant de mettre à jour les autorisations IAM, votre pipeline démarre et la mise à jour de la pile AWS CloudFormation rencontre des erreurs qui annulent la mise à jour de la pile. Si cela se produit, redémarrez votre pipeline après avoir corrigé les autorisations.

2. La mise à jour de la pile AWS CloudFormation démarre lorsque le pipeline de votre projet commence l'étape Déployer. Pour voir la notification de mise à jour de la pile lorsque le déploiement démarre, sur votre tableau de bord AWS CodeStar, sélectionnez l'étape AWS CloudFormation dans votre pipeline.

Pendant la mise à jour de la pile, AWS CloudFormation met automatiquement à jour les ressources du projet, comme suit :

- AWS CloudFormation traite le fichier `template.yml` en créant des fonctions Lambda disposant d'alias, des hooks d'événement et des ressources.
- AWS CloudFormation appelle Lambda pour créer la nouvelle version de la fonction.
- AWS CloudFormation crée un AppSpec fichier et appelle AWS CodeDeploy pour déplacer le trafic.

Pour plus d'informations sur la publication de fonctions Lambda aliasées dans SAM, consultez [AWS la référence du modèle d'application sans serveur \(SAM\)](#). Pour plus d'informations sur

les hooks d'événements et les ressources du AWS CodeDeploy AppSpec fichier, consultez la [section AppSpec « ressources » \(déploiements AWS Lambda uniquement\)](#) et la [section AppSpec « hooks » pour un déploiement AWS Lambda](#).

3. Une fois votre pipeline terminé, les ressources sont créées dans votre pile AWS CloudFormation. Sur la page Projet, dans la liste Ressources du projet, affichez l'application AWS CodeDeploy, le groupe de déploiement AWS CodeDeploy et les ressources de rôles de service AWS CodeDeploy créées pour votre projet.
4. Pour créer une nouvelle version, modifiez la fonction Lambda dans votre référentiel. Le nouveau déploiement démarre et déplace le trafic en fonction du type de déploiement indiqué dans le modèle SAM. Pour afficher le statut du trafic en cours de déplacement vers la nouvelle version, sur la page Projet, dans la liste Ressources du projet, choisissez le lien vers le déploiement AWS CodeDeploy.
5. Pour afficher les détails relatifs à chaque révision, sous Révisions, cliquez sur le lien du groupe de déploiement AWS CodeDeploy.
6. Dans votre répertoire de travail local, vous pouvez apporter des modifications à votre fonction AWS Lambda et valider la modification apportée à votre référentiel de projet. AWS CloudFormation prend en charge AWS CodeDeploy pour la gestion de la révision suivante de la même manière. Pour plus d'informations sur le redéploiement, l'arrêt ou l'annulation d'un déploiement Lambda, [consultez la section Déploiements sur une plate-forme de calcul AWS Lambda](#).

Transition de votre projet AWS CodeStar vers la production

Une fois que vous avez créé votre application à l'aide d'un projet AWS CodeStar et au vu du résultat fourni par AWS CodeStar, vous pouvez souhaiter passer votre projet à une utilisation en production. Pour ce faire, vous pouvez répliquer les données de votre application. AWS ressources en dehors d'AWS CodeStar. Vous aurez toujours besoin d'un référentiel, d'un projet de build, d'un pipeline et d'un déploiement, mais plutôt que de laisser AWS CodeStar les créer pour vous, vous les recréez à l'aide de. AWS CloudFormation.

Note

Il peut être utile de créer ou d'afficher un projet similaire en commençant par utiliser un démarrage rapide AWS CodeStar comme modèle pour votre propre projet, afin de vous assurer d'inclure les ressources et les stratégies dont vous avez besoin.

Un projet AWS CodeStar rassemble le code source et les ressources créées pour déployer le code. Les ressources qui, ensemble, aident à générer, publier et déployer le code sont appelées ressources de chaîne d'outils. Lors de la création d'un projet, un modèle AWS CloudFormation alloue les ressources de chaîne d'outils dans un pipeline d'intégration continue/de déploiement continu (CI/CD).

Lorsque vous utilisez la console pour créer un projet, le modèle de chaîne d'outils est créé pour vous. Lorsque vous utilisez l'AWS CLI pour créer un projet, vous créez le modèle de chaîne d'outils qui génère vos ressources de chaîne d'outils.

Une chaîne d'outils complète nécessite les ressources recommandées suivantes :

1. Un référentiel CodeCommit ou GitHub contenant votre code source.
2. Un pipeline CodePipeline configuré pour écouter les modifications apportées à votre référentiel.
 - a. Lorsque vous utilisez AWS CodeBuild pour exécuter des tests d'unité ou d'intégration, nous vous recommandons d'ajouter une étape de génération à votre pipeline pour créer des artefacts de génération.
 - b. Nous vous recommandons d'ajouter une étape de déploiement à votre pipeline qui utilise CodeDeploy ou AWS CloudFormation pour déployer les artefacts de génération et le code source dans votre infrastructure d'exécution.

Note

Sachant qu'un pipeline doit comporter au moins deux étapes dans un pipeline et que la première doit être l'étape source, ajoutez une étape de génération ou de déploiement en tant que deuxième étape.

Rubriques

- [Création d'un référentiel GitHub](#)

Création d'un référentiel GitHub

Vous créez un référentiel GitHub en le définissant dans votre modèle de chaîne d'outils. Assurez-vous que vous avez déjà créé un emplacement pour un fichier ZIP contenant votre code source, afin que le code puisse être chargé dans le référentiel. En outre, vous devez déjà avoir créé un jeton d'accès personnel dans GitHub, de sorte qu'AWS puisse se connecter à GitHub en votre

nom. En plus du jeton d'accès personnel pour GitHub, vous devez également avoir l'autorisation `s3.GetObject` pour l'objet Code que vous transmettez.

Pour spécifier un référentiel GitHub public, ajoutez le code suivant à votre modèle de chaîne d'outils dans AWS CloudFormation.

```
GitHubRepo:
Condition: CreateGitHubRepo
Description: GitHub repository for application source code
Properties:
  Code:
    S3:
      Bucket: MyCodeS3Bucket
      Key: MyCodeS3BucketKey
  EnableIssues: true
  IsPrivate: false
  RepositoryAccessToken: MyGitHubPersonalAccessToken
  RepositoryDescription: MyAppCodeRepository
  RepositoryName: MyAppSource
  RepositoryOwner: MyGitHubUserName
Type: AWS::CodeStar::GitHubRepository
```

Ce code spécifie les informations suivantes :

- L'emplacement du code que vous souhaitez inclure, qui doit être un compartiment Amazon S3.
- Si vous souhaitez activer les problèmes sur le référentiel GitHub.
- Si le référentiel GitHub est privé.
- Le jeton d'accès personnel GitHub que vous avez créé.
- Une description, un nom et un propriétaire pour le référentiel que vous créez.

Pour plus d'informations sur les informations à spécifier, consultez

le [AWS::CodeStar::GitHubRepository](#) dans le AWS CloudFormation Guide de l'utilisateur.

Utilisation des balises de projet dans AWS CodeStar

Vous pouvez associer des balises à des projets dans AWS CodeStar. Les balises peuvent vous aider à gérer vos projets. Par exemple, vous pouvez ajouter une balise avec une clé `Release` et une

valeur Beta à n'importe quel projet sur lequel travaille votre organisation en vue d'une future version bêta.

Ajout d'une balise à un projet

1. Le projet étant ouvert dans la AWS CodeStar console, dans le volet de navigation latéral, sélectionnez Paramètres.
2. Dans Tags, choisissez Modifier.
3. Dans Key, entrez le nom du tag. Dans Valeur, saisissez la valeur de la balise.
4. Facultatif : Choisissez Ajouter une étiquette pour ajouter d'autres balises.
5. Une fois que vous avez terminé d'ajouter des balises, choisissez Enregistrer.

Suppression d'une balise d'un projet

1. Le projet étant ouvert dans la AWS CodeStar console, dans le volet de navigation latéral, sélectionnez Paramètres.
2. Dans Tags, choisissez Modifier.
3. Dans Balises, recherchez la balise que vous souhaitez supprimer et choisissez Supprimer la balise.
4. Choisissez Save (Enregistrer).

Obtention de la liste de balises d'un projet

Utilisez l'AWS CLI pour exécuter la commande AWS CodeStar `list-tags-for-project`, en spécifiant le nom du projet :

```
aws codestar list-tags-for-project --id my-first-projec
```

En cas de réussite, une liste de balises similaire à ce qui suit s'affiche dans la sortie :

```
{
  "tags": {
    "Release": "Beta"
  }
}
```

Supprimer un projet AWS CodeStar

Si vous n'avez plus besoin d'un projet, vous pouvez le supprimer ainsi que ses ressources afin de ne pas engendrer de frais supplémentaires dans AWS. Lorsque vous supprimez un projet, tous les membres de l'équipe sont supprimés de ce projet. Leurs rôles de projet sont supprimés de leurs utilisateurs IAM, mais leurs profils utilisateur ne AWS CodeStar sont pas modifiés. Vous pouvez utiliser la console AWS CodeStar ou l'AWS CLI pour supprimer un projet. La suppression d'un projet nécessite le rôle de service AWS CodeStar, `aws-codestar-service-role`, qui doit être non modifié et assumable par AWS CodeStar.

Important

La suppression d'un projet AWS CodeStar est irréversible. Par défaut, toutes les ressources AWS du projet sont supprimées dans votre compte AWS, y compris :

- Le CodeCommit référentiel du projet ainsi que tout ce qui est stocké dans ce référentiel.
- Les rôles AWS CodeStar du projet et les politiques IAM associées configurés pour le projet et ses ressources.
- Toutes les instances Amazon EC2 créées pour le projet.
- L'application de déploiement et les ressources associées, telles que :
 - Une CodeDeploy application et les groupes de déploiement associés.
 - Une AWS Lambda fonction et les API API Gateway associées.
 - Une application AWS Elastic Beanstalk et l'environnement associé.
- Le pipeline de déploiement continu du projet dans CodePipeline.
- Les piles AWS CloudFormation associées au projet.
- Tout environnement de développement AWS Cloud9 créé avec la console AWS CodeStar. Toutes les modifications de code non enregistrées dans les environnements sont perdues.

Pour supprimer toutes les ressources du projet en même temps que le projet, cochez la case Supprimer les ressources. Si vous désactivez cette option, le projet est supprimé dans AWS CodeStar et les rôles de projet qui permettaient d'accéder à ces ressources sont supprimés dans IAM, mais toutes les autres ressources sont conservées. Vous voudrez peut-être continuer à vous acquitter de frais pour ces ressources dans AWS. Si vous décidez que vous n'avez plus besoin d'une ou de plusieurs de ces ressources, vous devez les supprimer

manuellement. Pour plus d'informations, veuillez consulter [Suppression de projet : un AWS CodeStar projet a été supprimé, mais les ressources existent toujours](#).

En tant que bonne pratique, si vous décidez de conserver les ressources lorsque vous supprimez un projet, copiez la liste des ressources sur la page des détails du projet. De cette façon, vous disposez d'un enregistrement de toutes les ressources conservées, même si le projet n'existe plus.

Rubriques

- [Supprimer un projet dans AWS CodeStar \(console\)](#)
- [Supprimer un projet dans AWS CodeStar \(AWS CLI\)](#)

Supprimer un projet dans AWS CodeStar (console)

Vous pouvez utiliser la console AWS CodeStar pour supprimer un projet.

Pour supprimer un projet dans AWS CodeStar

1. Ouvrez la AWS CodeStar console à l'[adresse https://console.aws.amazon.com/codestar/](https://console.aws.amazon.com/codestar/).
2. Choisissez Projets dans le volet de navigation.
3. Sélectionnez le projet que vous souhaitez supprimer, puis cliquez sur Supprimer.

Vous pouvez également ouvrir le projet et choisir Paramètres dans le volet de navigation situé sur le côté gauche de la console. Sur la page des détails du projet, choisissez Supprimer le projet.

4. Sur la page de confirmation de suppression, saisissez Supprimer. Maintenez l'option Supprimer les ressources sélectionnée si vous souhaitez supprimer les ressources du projet. Choisissez Delete (Supprimer).

Le processus de suppression d'un projet peut prendre plusieurs minutes. Une fois que le projet est supprimé, il ne s'affiche plus dans la liste des projets dans la console AWS CodeStar.

Important

Si votre projet utilise des ressources extérieures AWS (par exemple, un GitHub référentiel ou des problèmes dans Atlassian JIRA), ces ressources ne sont pas supprimées, même si vous cochez la case.

Votre projet ne peut pas être supprimé si des stratégies gérées AWS CodeStar ont été attachées manuellement à des rôles qui ne correspondent pas à des utilisateurs IAM. Si vous avez attaché l'une des stratégies gérées de votre projet au rôle d'un utilisateur fédéré, vous devez la détacher avant de pouvoir supprimer le projet. Pour plus d'informations, veuillez consulter [???](#).

Supprimer un projet dans AWS CodeStar (AWS CLI)

Vous pouvez utiliser l'AWS CLI pour supprimer un projet.

Pour supprimer un projet dans AWS CodeStar

1. Sur un terminal (Linux, macOS ou Unix) ou une invite de commande (Windows), exécutez la `delete-project` commande, y compris le nom du projet. Par exemple, pour supprimer un projet avec l'ID `my-2nd-project` :

```
aws codestar delete-project --id my-2nd-project
```

La sortie générée lors de l'exécution de cette commande est semblable à ce qui suit :

```
{
  "projectArn": "arn:aws:codestar:us-east-2:111111111111:project/my-2nd-project"
}
```

Les projets ne sont pas supprimés immédiatement.

2. Exécutez la commande `describe-project`, y compris le nom du projet. Par exemple, pour vérifier l'état d'un projet avec l'ID `my-2nd-project` :

```
aws codestar describe-project --id my-2nd-project
```

si le projet n'est pas encore supprimé, cette commande renvoie un résultat similaire au suivant :

```
{
  "name": "my project",
  "id": "my-2nd-project",
```



```
"arn": "arn:aws:codestar:us-west-2:123456789012:project/my-2nd-project",
"description": "My second CodeStar project.",
"createdTimeStamp": 1572547510.128,
"status": {
  "state": "CreateComplete"
}
}
```

Si le projet est supprimé, cette commande renvoie un résultat similaire au suivant :

```
An error occurred (ProjectNotFoundException) when calling the DescribeProject
operation: The project ID was not found: my-2nd-project. Make sure that the
project ID is correct and then try again.
```

3. Exécutez la commande `list-projects` et vérifiez que le projet supprimé n'apparaît plus dans la liste des projets associés à votre compte AWS.

```
aws codestar list-projects
```

Utilisation des équipes AWS CodeStar

Une fois que vous avez créé un projet de développement, vous devez en accorder l'accès à d'autres personnes pour pouvoir travailler avec elles. Dans AWS CodeStar, chaque projet a une équipe de projet. Un utilisateur peut appartenir à plusieurs projets AWS CodeStar et avoir différents rôles AWS CodeStar (et donc différentes autorisations) dans chacun de ces projets. Dans la console AWS CodeStar, les utilisateurs voient tous les projets associés à votre compte AWS, mais ne peuvent afficher et utiliser que les projets dans lesquels ils sont des membres d'équipe.

Les membres d'équipe peuvent se choisir un nom convivial. Ils peuvent également ajouter une adresse e-mail pour que les autres membres de l'équipe puissent les contacter. Les membres de l'équipe qui ne sont pas des propriétaires ne peuvent pas modifier leur rôle AWS CodeStar pour le projet.

Dans AWS CodeStar, chaque projet a trois rôles :

Rôles et autorisations dans un projet AWS CodeStar

Nom du rôle	Afficher le tableau de bord du projet et l'état du projet	Ajouter, supprimer des ressources de projet et accéder aux ressources de projet	Ajouter ou supprimer des membres de l'équipe	Supprimer le projet
Propriétaire	h/24, j/7	h/24, j/7	h/24, j/7	x
Participant	h/24, j/7	x		
Lecteur	h/24, j/7			

- **Propriétaire** : peut ajouter et supprimer d'autres membres de l'équipe, apporter du code à un référentiel de projet si le code est stocké CodeCommit, accorder ou refuser à d'autres membres de l'équipe l'accès à distance à toute instance Amazon EC2 exécutant Linux associée au projet, configurer le tableau de bord du projet et supprimer le projet.
- **Contributeur** : peut ajouter et supprimer des ressources de tableau de bord telles qu'une vignette JIRA, contribuer au référentiel du projet si le code y est stocké et interagir pleinement avec le

tableau de bord. CodeCommit Ne peut pas ajouter ou supprimer des membres de l'équipe, accorder ou refuser l'accès distant aux ressources ou supprimer le projet. C'est le rôle que vous devez choisir pour la plupart des membres de l'équipe.

- Afficheur : peut consulter le tableau de bord du projet, le code dans lequel il est stocké et CodeCommit, sur les vignettes du tableau de bord, l'état du projet et ses ressources.

Important

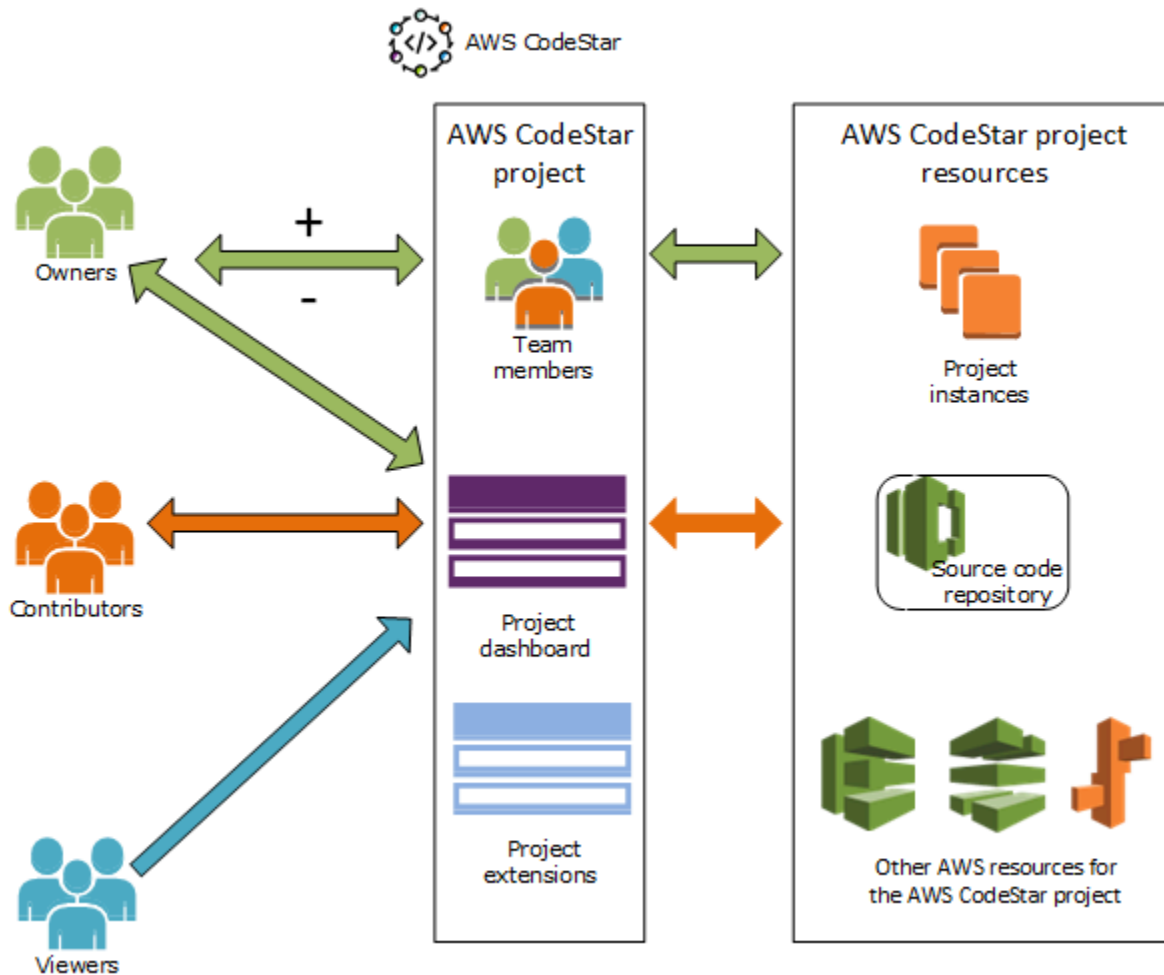
Si votre projet utilise des ressources extérieures AWS (par exemple, un GitHub référentiel ou des problèmes dans Atlassian JIRA), l'accès à ces ressources est contrôlé par le fournisseur de ressources, et non. AWS CodeStar Pour plus d'informations, référez-vous à la documentation du fournisseur de la ressource.

Toute personne ayant accès à un projet AWS CodeStar peut utiliser la console AWS CodeStar pour accéder à des ressources externes à AWS, mais qui sont associées à ce projet.

AWS CodeStar n'autorise pas automatiquement les membres de l'équipe de projet à participer aux environnements de développement AWS Cloud9 associés au projet. Pour autoriser un membre de l'équipe à participer à un environnement partagé, consultez [Partage d'un environnement AWS Cloud9 avec un membre de l'équipe de projet](#).

Une politique IAM est associée à chaque rôle du projet. Cette stratégie est personnalisée pour votre projet en vue de refléter ses ressources. Pour plus d'informations sur ces stratégies, consultez [AWS CodeStarExemples de politiques basées sur l'identité](#).

Le schéma suivant illustre la relation entre chaque rôle et un projet AWS CodeStar.



Rubriques

- [Ajouter des membres de l'équipe à un projet AWS CodeStar](#)
- [Gérer les autorisations pour les membres de l'équipe AWS CodeStar](#)
- [Supprimer des membres d'une équipe dans un projet AWS CodeStar](#)

Ajouter des membres de l'équipe à un projet AWS CodeStar

Si vous avez le rôle de propriétaire dans un AWS CodeStar projet ou si la `AWSCodeStarFullAccess` politique est appliquée à votre utilisateur IAM, vous pouvez ajouter d'autres utilisateurs IAM à l'équipe du projet. Il s'agit d'un processus simple qui applique un rôle AWS CodeStar (propriétaire, participant ou utilisateur) à l'utilisateur. Ces rôles sont propres à un projet et personnalisés. Par exemple, un membre de l'équipe disposant du rôle de participant dans un projet A peut ne pas bénéficier des mêmes autorisations sur les ressources qu'un membre de l'équipe disposant du rôle de participant dans un projet B. Un membre de l'équipe peut disposer

d'un seul rôle dans un projet. Une fois que vous avez ajouté un membre de l'équipe, il ou elle peut interagir immédiatement avec votre projet au niveau défini par le rôle.

Les avantages liés aux rôles AWS CodeStar et à l'appartenance à l'équipe sont les suivants :

- Il n'est pas nécessaire de configurer manuellement les autorisations dans IAM pour les membres de votre équipe.
- Vous pouvez facilement modifier le niveau d'accès d'un membre de l'équipe à un projet.
- Les utilisateurs peuvent accéder aux projets dans la AWS CodeStar console uniquement s'ils sont membres de l'équipe.
- L'accès des utilisateurs à un projet est défini par rôle.

Pour plus d'informations sur les équipes et les rôles AWS CodeStar, consultez [Utilisation des équipes AWS CodeStar](#) et [Utilisation de votre profil utilisateur AWS CodeStar](#).

Pour ajouter un membre de l'équipe à un projet, vous devez disposer du rôle de propriétaire AWS CodeStar pour le projet ou la stratégie `AWSCodeStarFullAccess` doit être appliquée.

Important

L'ajout d'un membre de l'équipe n'affecte pas l'accès de ce membre aux ressources situées en dehors de AWS (par exemple, un GitHub référentiel ou des problèmes dans Atlassian JIRA). Ces autorisations d'accès sont contrôlées par le fournisseur des ressources, pas AWS CodeStar. Pour plus d'informations, référez-vous à la documentation du fournisseur de la ressource.

Toute personne ayant accès à un AWS CodeStar projet peut utiliser la AWS CodeStar console pour accéder à des ressources extérieures à ce projet AWS, mais qui y sont liées. L'ajout d'un membre de l'équipe à un projet n'autorise pas automatiquement ce dernier à participer aux environnements de développement AWS Cloud9 associés du projet. Pour autoriser un membre de l'équipe à participer à un environnement partagé, consultez [Partage d'un environnement AWS Cloud9 avec un membre de l'équipe de projet](#).

Accorder à un utilisateur fédéré l'accès à un projet implique d'attacher manuellement la stratégie de propriétaire, participant ou utilisateur AWS CodeStar au rôle endossé par l'utilisateur fédéré. Pour plus d'informations, veuillez consulter [Accès utilisateur fédéré à AWS CodeStar](#).

Rubriques

- [Ajouter un membre d'équipe \(Console\)](#)
- [Ajouter et afficher des membres de l'équipe \(AWS CLI\)](#)

Ajouter un membre d'équipe (Console)

Vous pouvez utiliser la console AWS CodeStar pour ajouter un membre à votre équipe de projet. Si un utilisateur IAM existe déjà pour la personne que vous souhaitez ajouter, vous pouvez ajouter cet utilisateur IAM. Sinon, vous pouvez créer un utilisateur IAM pour cette personne lorsque vous l'ajoutez à votre projet.

Pour ajouter un membre de l'équipe à un projet AWS CodeStar (console)

1. Ouvrez la AWS CodeStar console à l'[adresse https://console.aws.amazon.com/codestar/](https://console.aws.amazon.com/codestar/).
2. Choisissez Projets dans le volet de navigation et choisissez votre projet.
3. Dans le volet de navigation latéral du projet, choisissez Team.
4. Sur la page Team members (Membres d'équipe), choisissez Ajouter un membre d'équipe.
5. Dans Choose user (Choisir un utilisateur), effectuez l'une des actions suivantes :
 - Si un utilisateur IAM existe déjà pour la personne que vous souhaitez ajouter, choisissez-le dans la liste.

Note

Les utilisateurs qui ont déjà été ajoutés à un autre AWS CodeStar projet apparaissent dans la liste des AWS CodeStar utilisateurs existants.

Dans Rôle du projet, choisissez le AWS CodeStar rôle (propriétaire, contributeur ou spectateur) de cet utilisateur. C'est un rôle de niveau projet AWS CodeStar qui ne peut être modifié que par un propriétaire du projet. Lorsqu'il est appliqué à un utilisateur IAM, le rôle fournit toutes les autorisations requises pour accéder aux ressources AWS CodeStar du projet. Il applique les politiques requises pour créer et gérer les informations d'identification Git pour le code stocké CodeCommit dans IAM ou pour télécharger les clés SSH Amazon EC2 pour l'utilisateur dans IAM.

⚠ Important

Vous ne pouvez pas fournir ou modifier le nom d'affichage ou les informations de courrier électronique d'un utilisateur IAM à moins d'être connecté à la console en tant qu'utilisateur. Pour plus d'informations, veuillez consulter [Gérer les informations d'affichage pour votre profil utilisateur AWS CodeStar](#).

Choisissez Ajouter un membre de l'équipe.

- S'il n'existe pas d'utilisateur IAM pour la personne que vous souhaitez ajouter au projet, choisissez Créer un nouvel utilisateur IAM. Vous serez redirigé vers la console IAM où vous pourrez créer un nouvel utilisateur IAM. Pour plus d'informations, reportez-vous à la section [Création d'utilisateurs IAM](#) dans le guide de l'utilisateur IAM. Après avoir créé votre utilisateur IAM, revenez à la AWS CodeStar console, actualisez la liste des utilisateurs et choisissez l'utilisateur IAM que vous avez créé dans la liste déroulante. Entrez le nom AWS CodeStar d'affichage, l'adresse e-mail et le rôle de projet que vous souhaitez appliquer à ce nouvel utilisateur, puis choisissez Ajouter un membre de l'équipe.

ℹ Note

Pour faciliter la gestion, le rôle Propriétaire doit être attribué à au moins un utilisateur du projet.

6. Envoyez les informations suivantes au nouveau membre de l'équipe :

- Informations de connexion pour votre projet AWS CodeStar.
- Si le code source est stocké dans CodeCommit des [instructions pour configurer l'accès au CodeCommit référentiel à l'aide des informations d'identification Git](#) à partir de leurs ordinateurs locaux.
- Informations sur la façon dont l'utilisateur peut gérer son nom d'affichage, son adresse e-mail et sa clé SSH publique Amazon EC2, comme décrit dans. [Utilisation de votre profil utilisateur AWS CodeStar](#)
- Mot de passe et informations de connexion à usage unique, si l'utilisateur est nouveau AWS et que vous avez créé un utilisateur IAM pour cette personne. Le mot de passe expire à la première connexion de l'utilisateur. L'utilisateur doit choisir un nouveau mot de passe.

Ajouter et afficher des membres de l'équipe (AWS CLI)

Vous pouvez utiliser l'AWS CLI pour ajouter des membres à votre équipe de projet. Vous pouvez également afficher des informations sur tous les membres de l'équipe de votre projet.

Pour ajouter un membre d'équipe

1. Ouvrez une fenêtre de terminal ou de commande.
2. Exécutez la commande `associate-team-member` avec les paramètres `--project-id`, `-user-arn` et `--project-role`. Vous pouvez également spécifier si l'utilisateur dispose d'un accès à distance aux instances du projet en incluant les paramètres `--remote-access-allowed` ou `--no-remote-access-allowed`. Par exemple :

```
aws codestar associate-team-member --project-id my-first-projec --user-arn
arn:aws:iam:111111111111:user/Jane_Doe --project-role Contributor --remote-access-
allowed
```

Cette commande ne renvoie aucun résultat.

Pour afficher tous les membres de l'équipe (AWS CLI)

1. Ouvrez une fenêtre de terminal ou de commande.
2. Exécutez la commande `list-team-members` avec le paramètre `--project-id`. Par exemple :

```
aws codestar list-team-members --project-id my-first-projec
```

La sortie générée lors de l'exécution de cette commande est semblable à ce qui suit :

```
{
  "teamMembers": [
    {"projectRole": "Owner", "remoteAccessAllowed": true, "userArn": "arn:aws:iam::111111111111:use
Mary_Major"},
    {"projectRole": "Contributor", "remoteAccessAllowed": true, "userArn": "arn:aws:iam::1111111111
Jane_Doe"},
    {"projectRole": "Contributor", "remoteAccessAllowed": true, "userArn": "arn:aws:iam::1111111111
John_Doe"},
```



```
{ "projectRole": "Viewer", "remoteAccessAllowed": false, "userArn": "arn:aws:iam::111111111111:u  
John_Stiles" }  
]  
}
```

Gérer les autorisations pour les membres de l'équipe AWS CodeStar

Vous modifiez des autorisations pour les membres de l'équipe en changeant leur rôle AWS CodeStar. Chaque membre de l'équipe peut être affecté à un seul rôle dans un projet AWS CodeStar, mais de plusieurs utilisateurs peuvent être affectés au même rôle. Vous ne pouvez pas utiliser la console AWS CodeStar ou AWS CLI pour gérer les autorisations.

Important

Pour modifier un rôle pour un membre de l'équipe, vous devez disposer du rôle de propriétaire AWS CodeStar pour ce projet ou la stratégie `AWSCodeStarFullAccess` doit être appliquée.

La modification des autorisations d'un membre de l'équipe n'affecte pas l'accès de ce membre à des ressources situées en dehors de AWS (par exemple, un GitHub référentiel ou des problèmes dans Atlassian JIRA). Ces autorisations d'accès sont contrôlées par le fournisseur des ressources, pas AWS CodeStar. Pour plus d'informations, référez-vous à la documentation du fournisseur de la ressource.

Toute personne ayant accès à un projet AWS CodeStar peut être en mesure d'utiliser la console AWS CodeStar pour accéder à des ressources en dehors d'AWS, mais qui sont associées à ce projet.

Le fait de modifier le rôle d'un membre d'équipe pour un projet n'autorise pas automatiquement ce membre à participer à des environnements de développement AWS Cloud9 pour le projet. Pour autoriser un membre de l'équipe à participer à un environnement partagé ou l'en empêcher, consultez [Partage d'un environnement AWS Cloud9 avec un membre de l'équipe de projet](#).

Vous pouvez également autoriser les utilisateurs à accéder à distance à toutes les instances Linux Amazon EC2 associées au projet. Après avoir accordé cette autorisation, l'utilisateur doit charger une clé publique SSH associée à son profil utilisateur AWS CodeStar dans tous les projets de l'équipe.

Pour se connecter correctement aux instances Linux, l'utilisateur doit avoir configuré SSH et la clé privée sur l'ordinateur local.

Rubriques

- [Gérer les autorisations de l'équipe \(Console\)](#)
- [Gérer les autorisations de l'équipe \(AWS CLI\)](#)

Gérer les autorisations de l'équipe (Console)

Vous pouvez utiliser la console AWS CodeStar pour gérer les rôles des membres de l'équipe. Vous pouvez également déterminer si les membres de l'équipe ont accès à distance aux instances Amazon EC2 associées à votre projet.

Pour modifier le rôle d'un membre de l'équipe

1. Ouvrez la AWS CodeStar console à l'[adresse https://console.aws.amazon.com/codestar/](https://console.aws.amazon.com/codestar/).
2. Choisissez Projets dans le volet de navigation et choisissez votre projet.
3. Dans le volet de navigation latéral du projet, choisissez Team.
4. Sur la page Membres de l'équipe, choisissez le membre de l'équipe, puis sélectionnez Modifier.
5. Dans Rôle du projet, choisissez le AWS CodeStar rôle (propriétaire, contributeur ou téléspectateur) que vous souhaitez attribuer à cet utilisateur.

Pour plus d'informations sur les rôles AWS CodeStar et leurs autorisations, consultez [Utilisation des équipes AWS CodeStar](#).

Choisissez Modifier le membre de l'équipe.

Pour accorder à un membre de l'équipe des autorisations d'accès à distance aux instances Amazon EC2

1. Ouvrez la AWS CodeStar console à l'[adresse https://console.aws.amazon.com/codestar/](https://console.aws.amazon.com/codestar/).
2. Choisissez Projets dans le volet de navigation et choisissez votre projet.
3. Dans le volet de navigation latéral du projet, choisissez Team.
4. Sur la page Membres de l'équipe, choisissez le membre de l'équipe, puis sélectionnez Modifier.
5. Sélectionnez Autoriser l'accès SSH aux instances du projet, puis sélectionnez Modifier le membre de l'équipe.

6. (Facultatif) Avertissez les membres de l'équipe qu'ils doivent charger une clé publique SSH pour leurs utilisateurs AWS CodeStar, si ce n'est déjà fait. Pour plus d'informations, veuillez consulter [Ajouter une clé publique à votre profil AWS CodeStar utilisateur](#).

Gérer les autorisations de l'équipe (AWS CLI)

Vous pouvez utiliser AWS CLI pour gérer le rôle de projet affecté à un membre de l'équipe. Vous pouvez utiliser les mêmes AWS CLI commandes pour déterminer si ce membre de l'équipe dispose d'un accès à distance aux instances Amazon EC2 associées à votre projet.

Pour gérer les autorisations d'un membre de l'équipe

1. Ouvrez une fenêtre de terminal ou de commande.
2. Exécutez la commande `update-team-member` avec les paramètres `--project-id`, `--user-arn` et `--project-role`. Vous pouvez également spécifier si l'utilisateur dispose d'un accès à distance aux instances du projet en incluant les paramètres `--remote-access-allowed` ou `--no-remote-access-allowed`. Par exemple, pour mettre à jour le rôle de projet d'un utilisateur IAM nommé `John_Doe` et modifier ses autorisations en tant que visionneur n'ayant aucun accès à distance aux instances du projet Amazon EC2 :

```
aws codestar update-team-member --project-id my-first-projec --user-arn
arn:aws:iam:111111111111:user/John_Doe --project-role Viewer --no-remote-access-
allowed
```

La sortie générée lors de l'exécution de cette commande est semblable à ce qui suit :

```
{
  "projectRole": "Viewer",
  "remoteAccessAllowed": false,
  "userArn": "arn:aws:iam::111111111111:user/John_Doe"
}
```

Supprimer des membres d'une équipe dans un projet AWS CodeStar

Une fois que vous avez supprimé un utilisateur d'un AWS CodeStar projet, celui-ci apparaît toujours dans l'historique des validations du référentiel du projet, mais n'a plus accès au CodeCommit

référentiel ni à aucune autre ressource du projet, telle que le pipeline du projet. (L'exception à cette règle concerne un utilisateur IAM qui dispose d'autres politiques autorisant l'accès à ces ressources.) L'utilisateur ne peut pas accéder au tableau de bord du projet, et le projet n'apparaît plus dans la liste des projets qu'il voit sur le AWS CodeStar tableau de bord. Vous pouvez utiliser la console AWS CodeStar ou AWS CLI pour supprimer des membres de votre équipe de projet.

Important

Bien que le retrait d'un membre de l'équipe d'un projet empêche l'accès à distance aux instances Amazon EC2 du projet, cela ne ferme aucune des sessions SSH actives de l'utilisateur.

La suppression d'un membre de l'équipe n'affecte pas l'accès de ce membre à des ressources extérieures AWS (par exemple, un GitHub référentiel ou des problèmes dans Atlassian JIRA). Ces autorisations d'accès sont contrôlées par le fournisseur des ressources, pas AWS CodeStar. Pour plus d'informations, référez-vous à la documentation du fournisseur de la ressource.

La suppression d'un membre d'équipe d'un projet ne supprime pas automatiquement les environnements de développement AWS Cloud9 relatifs à ce membre et n'empêche pas ce membre de participer à des environnements de développement AWS Cloud9 associés auxquels il a été invité. Pour supprimer un environnement de développement, consultez [Suppression d'un environnement AWS Cloud9 d'un projet](#). Pour empêcher un membre de l'équipe à participer à un environnement partagé, consultez [Partage d'un environnement AWS Cloud9 avec un membre de l'équipe de projet](#).

Pour supprimer un membre de l'équipe d'un projet, vous devez disposer du rôle de propriétaire AWS CodeStar pour ce projet, ou bien la stratégie `AWSCodeStarFullAccess` doit être appliquée à votre compte.

Rubriques

- [Supprimer des membres de l'équipe \(Console\)](#)
- [Supprimer des membre de l'équipe \(AWS CLI\)](#)

Supprimer des membres de l'équipe (Console)

Vous pouvez utiliser la console AWS CodeStar pour supprimer des membres de votre équipe de projet.

Pour supprimer un membre de l'équipe dans un projet

1. Ouvrez la AWS CodeStar console à l'[adresse https://console.aws.amazon.com/codestar/](https://console.aws.amazon.com/codestar/).
2. Choisissez Projets dans le volet de navigation et choisissez votre projet.
3. Dans le volet de navigation latéral du projet, choisissez Team.
4. Sur la page Membres de l'équipe, choisissez le membre de l'équipe, puis sélectionnez Supprimer.

Supprimer des membre de l'équipe (AWS CLI)

Vous pouvez utiliser AWS CLI pour supprimer des membres de votre équipe de projet.

Pour supprimer un membre de l'équipe

1. Ouvrez une fenêtre de terminal ou de commande.
2. Exécutez la commande `disassociate-team-member` avec les paramètres `--project-id` et `-user-arn`. Par exemple :

```
aws codestar disassociate-team-member --project-id my-first-projec --user-arn
arn:aws:iam:111111111111:user/John_Doe
```

La sortie générée lors de l'exécution de cette commande est semblable à ce qui suit :

```
{
  "projectId": "my-first-projec",
  "userArn": "arn:aws:iam::111111111111:user/John_Doe"
}
```

Utilisation de votre profil utilisateur AWS CodeStar

Votre profil AWS CodeStar utilisateur est associé à votre utilisateur IAM. Ce profil contient un nom d'affichage et une adresse e-mail qui est utilisée dans tous les projets AWS CodeStar auxquels vous appartenez. Vous pouvez charger une clé publique SSH à associer à votre profil. Cette clé publique fait partie de la paire de clés SSH publique-privée que vous utilisez lorsque vous vous connectez aux instances Amazon EC2 AWS CodeStar associées aux projets auxquels vous appartenez.

Note

Les informations de ces sections couvrent uniquement votre profil utilisateur AWS CodeStar. Si votre projet utilise des ressources extérieures AWS (par exemple, un GitHub référentiel ou des problèmes dans Atlassian JIRA), ces fournisseurs de ressources peuvent utiliser leurs propres profils utilisateur, qui peuvent avoir des paramètres différents. Pour plus d'informations, référez-vous à la documentation du fournisseur de la ressource.

Rubriques

- [Gérer les informations d'affichage pour votre profil utilisateur AWS CodeStar](#)
- [Ajouter une clé publique à votre profil AWS CodeStar utilisateur](#)

Gérer les informations d'affichage pour votre profil utilisateur AWS CodeStar

Vous pouvez utiliser la console AWS CodeStar ou AWS CLI pour modifier le nom d'affichage et l'adresse e-mail dans votre profil utilisateur. Un profil utilisateur n'est pas spécifique au projet. Il est associé à votre utilisateur IAM et est appliqué à tous les AWS CodeStar projets auxquels vous appartenez dans une AWS région. Si vous appartenez à des projets dans plusieurs régions AWS, vous aurez des profils utilisateur distincts.

Vous ne pouvez gérer que votre propre profil utilisateur dans la console AWS CodeStar. Si vous disposez de la stratégie `AWSCodeStarFullAccess`, vous pouvez utiliser AWS CLI pour afficher et gérer d'autres profils.

 Note


Les informations de cette section couvrent uniquement votre profil utilisateur AWS CodeStar. Si votre projet utilise des ressources extérieures AWS (par exemple, un GitHub référentiel ou des problèmes dans Atlassian JIRA), ces fournisseurs de ressources peuvent utiliser leurs propres profils utilisateur, qui peuvent avoir des paramètres différents. Pour plus d'informations, référez-vous à la documentation du fournisseur de la ressource.

Rubriques

- [Gérer votre profil utilisateur \(Console\)](#)
- [Gérer les profils utilisateur \(AWS CLI\)](#)

Gérer votre profil utilisateur (Console)

Vous pouvez gérer votre profil utilisateur dans la console AWS CodeStar en accédant à un projet dans lequel vous êtes un membre d'équipe et en changeant vos informations de profil. Étant donné que les profils utilisateur sont spécifiques à l'utilisateur et non au projet, les modifications de votre profil utilisateur apparaissent dans chaque projet d'une région AWS où vous êtes un membre d'équipe.

 Important

Pour utiliser la console afin de modifier les informations d'affichage d'un utilisateur, vous devez être connecté en tant qu'utilisateur IAM. Aucun autre utilisateur, même ceux ayant un rôle de propriétaire AWS CodeStar pour un projet ou avec la stratégie `AWSCodeStarFullAccess` appliquée, ne peut changer vos informations d'affichage.

Pour modifier vos informations d'affichage dans tous les projets dans une région AWS

1. Ouvrez la AWS CodeStar console à l'[adresse https://console.aws.amazon.com/codestar/](https://console.aws.amazon.com/codestar/).
2. Choisissez Projets dans le volet de navigation et choisissez un projet dans lequel vous faites partie de l'équipe.
3. Dans le volet de navigation latéral du projet, choisissez Team.
4. Sur la page Membres de l'équipe, choisissez l'utilisateur IAM, puis sélectionnez Modifier.

5. Modifiez le nom d'affichage, l'adresse e-mail, ou les deux, puis choisissez Modifier le membre de l'équipe.

 Note

Un nom d'affichage et une adresse e-mail sont obligatoires. Pour plus d'informations, veuillez consulter [Limites dans AWS CodeStar](#).

Gérer les profils utilisateur (AWS CLI)

Vous pouvez utiliser AWS CLI pour créer et gérer votre profil utilisateur dans AWS CodeStar. Vous pouvez également utiliser AWS CLI pour afficher les informations de votre profil utilisateur et tous les profils utilisateur configurés pour votre compte AWS dans une région AWS.

Assurez-vous que votre AWS profil est configuré pour la région dans laquelle vous souhaitez créer, gérer ou consulter les profils utilisateur.

Pour créer un profil utilisateur

1. Ouvrez une fenêtre de terminal ou de commande.
2. Exécutez la commande `create-user-profile` avec les paramètres `user-arn`, `display-name` et `email-address`. Par exemple :

```
aws codestar create-user-profile --user-arn arn:aws:iam:111111111111:user/John_Stiles --display-name "John Stiles" --email-address "john_stiles@example.com"
```

La sortie générée lors de l'exécution de cette commande est semblable à ce qui suit :

```
{
  "createdTimestamp":1.491439687681E9,
  "displayName":"John Stiles",
  "emailAddress":"john.stiles@example.com",
  "lastModifiedTimestamp":1.491439687681E9,
  "userArn":"arn:aws:iam::111111111111:user/Jane_Doe"
}
```


Pour afficher vos informations d'affichage

1. Ouvrez une fenêtre de terminal ou de commande.
2. Exécutez la commande `describe-user-profile` avec le paramètre `user-arn`. Par exemple :

```
aws codestar describe-user-profile --user-arn arn:aws:iam:111111111111:user/
Mary_Major
```

La sortie générée lors de l'exécution de cette commande est semblable à ce qui suit :

```
{
  "createdTimestamp":1.490634364532E9,
  "displayName":"Mary Major",
  "emailAddress":"mary.major@example.com",
  "lastModifiedTimestamp":1.491001935261E9,
  "sshPublicKey":"EXAMPLE=",
  "userArn":"arn:aws:iam::111111111111:user/Mary_Major"
}
```

Pour modifier vos informations d'affichage

1. Ouvrez une fenêtre de terminal ou de commande.
2. Exécutez la commande `update-user-profile` avec le paramètre `user-arn` et les paramètres de profil que vous voulez modifier, par exemple `display-name` ou `email-address`. Par exemple, si un utilisateur ayant le nom d'affichage Jane Doe souhaite remplacer son nom d'affichage par Jane Mary Doe :

```
aws codestar update-user-profile --user-arn arn:aws:iam:111111111111:user/Jane_Doe
--display-name "Jane Mary Doe"
```

La sortie générée lors de l'exécution de cette commande est semblable à ce qui suit :

```
{
  "createdTimestamp":1.491439687681E9,
  "displayName":"Jane Mary Doe",
  "emailAddress":"jane.doe@example.com",
  "lastModifiedTimestamp":1.491442730598E9,
  "sshPublicKey":"EXAMPLE1",
  "userArn":"arn:aws:iam::111111111111:user/Jane_Doe"
```

```
}
```

Pour répertorier tous les profils utilisateur d'une région AWS dans votre compte AWS

1. Ouvrez une fenêtre de terminal ou de commande.
2. Exécutez la commande `aws codestar list-user-profiles`. Par exemple :

```
aws codestar list-user-profiles
```

La sortie générée lors de l'exécution de cette commande est semblable à ce qui suit :

```
{
  "userProfiles":[
    {
      "displayName":"Jane Doe",
      "emailAddress":"jane.doe@example.com",
      "sshPublicKey":"EXAMPLE1",
      "userArn":"arn:aws:iam::111111111111:user/Jane_Doe"
    },
    {
      "displayName":"John Doe",
      "emailAddress":"john.doe@example.com",
      "sshPublicKey":"EXAMPLE2",
      "userArn":"arn:aws:iam::111111111111:user/John_Doe"
    },
    {
      "displayName":"Mary Major",
      "emailAddress":"mary.major@example.com",
      "sshPublicKey":"EXAMPLE=",
      "userArn":"arn:aws:iam::111111111111:user/Mary_Major"
    },
    {
      "displayName":"John Stiles",
      "emailAddress":"john.stiles@example.com",
      "sshPublicKey":"",
      "userArn":"arn:aws:iam::111111111111:user/John_Stiles"
    }
  ]
}
```

Ajouter une clé publique à votre profil AWS CodeStar utilisateur

Vous pouvez charger une clé SSH publique faisant partie de la paire de clés publique-privée que vous créez et gérez. Vous utilisez cette paire de clés SSH publique-privée pour accéder aux instances Amazon EC2 exécutant Linux. Si un propriétaire de projet vous a accordé une autorisation d'accès distant, vous ne pouvez accéder qu'aux instances associées au projet. Vous pouvez utiliser la AWS CodeStar console ou AWS CLI gérer votre clé publique.

Important

Un propriétaire de AWS CodeStar projet peut accorder aux propriétaires de projet, aux contributeurs et aux spectateurs un accès SSH aux instances Amazon EC2 pour le projet, mais seule la personne (propriétaire, contributeur ou téléspectateur) peut définir la clé SSH. Pour ce faire, il doit être connecté en tant que propriétaire, participant ou utilisateur individuel. AWS CodeStar ne gère pas les clés SSH pour les AWS Cloud9 environnements.

Rubriques

- [Gérer votre clé publique \(console\)](#)
- [Gérer votre clé publique \(AWS CLI\)](#)
- [Connectez-vous à une instance Amazon EC2 avec votre clé privée](#)

Gérer votre clé publique (console)

Bien que vous ne puissiez pas générer de paire de clés publique-privée dans la console, vous pouvez en créer une localement, puis l'ajouter ou la gérer dans le cadre de votre profil utilisateur via la AWS CodeStar console.

Pour gérer votre clé SSH publique

1. Dans une fenêtre de terminal ou d'émulateur Bash, exécutez la commande `ssh-keygen` pour générer une paire de clés publique-privée SSH sur votre ordinateur local. Vous pouvez générer une clé dans n'importe quel format autorisé par Amazon EC2. Pour plus d'informations sur les formats acceptables, consultez [Importation de votre propre clé publique sur Amazon EC2](#). L'idéal est de générer une clé SSH-2 RSA, au format OpenSSH et contenant 2 048 bits. La clé publique est stockée dans un fichier avec l'extension `.pub`.
2. Ouvrez la AWS CodeStar console à l'[adresse https://console.aws.amazon.com/codestar/](https://console.aws.amazon.com/codestar/).

Choisissez un projet où vous êtes un membre de l'équipe.

3. Dans le volet de navigation, choisissez Team.
4. Sur la page Membres de l'équipe, recherchez le nom de votre utilisateur IAM, puis choisissez Modifier.
5. Sur la page Modifier un membre de l'équipe, sous Accès à distance, activez Autoriser l'accès SSH aux instances du projet.
6. Dans le champ Clé publique SSH, collez la clé publique, puis choisissez Modifier le membre de l'équipe.

Note

Vous pouvez modifier votre clé publique en supprimant l'ancienne clé dans ce champ et en collant une nouvelle clé. Vous pouvez supprimer une clé publique en supprimant le contenu de ce champ, puis en choisissant Modifier le membre de l'équipe.

Lorsque vous modifiez ou supprimez une clé publique, vous modifiez votre profil utilisateur. Ce n'est pas une modification spécifique au projet. Étant donné que votre clé est associée à votre profil, elle change (ou est supprimée) dans tous les projets pour lesquels un accès distant vous a été accordé.

La suppression de votre clé publique supprime votre accès aux instances Amazon EC2 exécutant Linux dans tous les projets pour lesquels un accès à distance vous a été accordé. Par contre, les sessions SSH ouvertes utilisant cette clé ne sont pas fermées. Veillez à fermer toutes les sessions ouvertes.

Gérer votre clé publique (AWS CLI)

Vous pouvez utiliser le AWS CLI pour gérer votre clé publique SSH dans le cadre de votre profil utilisateur.

Pour gérer votre clé publique

1. Dans une fenêtre de terminal ou d'émulateur Bash, exécutez la commande `ssh-keygen` pour générer une paire de clés publique-privée SSH sur votre ordinateur local. Vous pouvez générer une clé dans n'importe quel format autorisé par Amazon EC2. Pour plus d'informations sur les

formats acceptables, consultez [Importation de votre propre clé publique sur Amazon EC2](#). L'idéal est de générer une clé SSH-2 RSA, au format OpenSSH et contenant 2 048 bits. La clé publique est stockée dans un fichier avec l'extension `.pub`.

2. Pour ajouter ou modifier votre clé publique SSH dans votre profil AWS CodeStar utilisateur, exécutez la `update-user-profile` commande avec le `--ssh-public-key` paramètre. Par exemple :

```
aws codestar update-user-profile --user-arn arn:aws:iam:111111111111:user/Jane_Doe
--ssh-key-id EXAMPLE1
```

La sortie générée lors de l'exécution de cette commande est semblable à ce qui suit :

```
{
  "createdTimestamp":1.491439687681E9,
  "displayName":"Jane Doe",
  "emailAddress":"jane.doe@example.com",
  "lastModifiedTimestamp":1.491442730598E9,
  "sshPublicKey":"EXAMPLE1",
  "userArn":"arn:aws:iam::111111111111:user/Jane_Doe"
}
```

Connectez-vous à une instance Amazon EC2 avec votre clé privée

Assurez-vous d'avoir créé une paire de clés Amazon EC2. Ajoutez votre clé publique à votre profil utilisateur dans AWS CodeStar. Pour créer une paire de clés, consultez [Étape 4 : Création d'une paire de clés Amazon EC2 pour les projets AWS CodeStar](#). Pour ajouter votre clé publique à votre profil utilisateur, consultez les instructions fournies plus haut dans cette rubrique.

Pour vous connecter à une instance Linux Amazon EC2 à l'aide de votre clé privée

1. Votre projet étant ouvert dans la AWS CodeStar console, dans le volet de navigation, sélectionnez **Projet**.
2. Dans **Ressources** du projet, choisissez le lien **ARN** dans la ligne où le type est **Amazon EC2** et le nom commence par **instance**.
3. Dans la console Amazon EC2, choisissez **Connect**.
4. Suivez les instructions indiquées dans la boîte de dialogue **Connect To Your Instance** (Connectez-vous à votre instance).

Pour le nom d'utilisateur, utilisez `ec2-user`. Si vous n'utilisez pas le nom d'utilisateur correct, vous ne pouvez pas vous connecter à l'instance.

Pour plus d'informations, consultez les ressources suivantes dans le guide de l'utilisateur Amazon EC2.

- [Connexion à votre instance Linux à l'aide de SSH](#)
- [Connexion à votre instance Linux à partir de Windows à l'aide de PuTTY](#)
- [Connexion à votre instance Linux à l'aide de MindTerm](#)

Sécurité dans AWS CodeStar

Chez AWS, la sécurité dans le cloud est notre priorité numéro 1. En tant que client AWS, vous bénéficiez d'un centre de données et d'une architecture réseau conçus pour répondre aux exigences des organisations les plus pointilleuses en termes de sécurité.

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

- Sécurité du cloud : AWS est responsable de la protection de l'infrastructure qui exécute des services AWS dans le cloud AWS. AWS vous fournit également les 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 [AWSconformité Programmes](#) de conformité. Pour en savoir plus sur les programmes de conformité qui s'appliquent à AWS CodeStar, veuillez consulter la rubrique [Services AWS concernés par le programme de conformité](#).
- Sécurité dans le cloud : votre responsabilité est déterminée par le service AWS que vous utilisez. Vous êtes également responsable d'autres facteurs, y compris de la sensibilité de vos données, des exigences de votre entreprise, ainsi que de la législation et de la réglementation applicables.

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

Lorsque vous créez des politiques personnalisées et que vous utilisez des limites d'autorisation AWS CodeStar, gardez un accès avec le moindre privilège en n'accordant que les autorisations nécessaires à l'exécution d'une tâche et en limitant les autorisations aux ressources ciblées. Pour empêcher les membres d'autres projets d'accéder aux ressources de votre projet, accordez aux membres de l'organisation des autorisations distinctes pour chaque AWS CodeStar projet. Il est recommandé de créer un compte de projet pour chaque membre, puis d'attribuer un accès basé sur les rôles à ce compte.

Par exemple, vous pouvez utiliser un service tel que AWS Control Tower with AWS Organizations pour créer des comptes pour chaque rôle de développeur au sein d'un DevOps groupe. Vous pouvez ensuite attribuer des autorisations à ces comptes. Les autorisations générales s'appliquent au compte, mais l'utilisateur dispose d'un accès limité aux ressources extérieures au projet.

Pour plus d'informations sur la gestion de l'accès au moindre privilège aux AWS ressources à l'aide d'une stratégie multi-comptes, reportez-vous à la stratégie [multi-comptes AWS pour votre zone de landing zone dans le guide de l'utilisateur](#) de AWSControl Tower.

Rubriques

- [Protection des données dans AWS CodeStar](#)
- [Identity and Access Management \(IAM\) pour AWS CodeStar](#)
- [Journalisation des AWS CodeStar appels d'API avec AWS CloudTrail](#)
- [Validation de la conformité pour AWS CodeStar](#)
- [Résilience dans AWS CodeStar](#)
- [Sécurité de l'infrastructure dans AWS CodeStar](#)

Protection des données dans AWS CodeStar

Le [modèle de responsabilité AWS partagée](#) de s'applique à la protection des données dans AWS CodeStar. Comme décrit dans ce modèle, AWS est chargé de protéger l'infrastructure mondiale qui gère tous les AWS Cloud. La gestion du contrôle de votre contenu hébergé sur cette infrastructure relève de votre responsabilité. Vous êtes également responsable des tâches de configuration et de gestion de la sécurité des Services AWS que vous utilisez. Pour plus d'informations sur la confidentialité des données, consultez la section [Confidentialité des données FAQ](#). Pour plus d'informations sur la protection des données en Europe, consultez le [modèle de responsabilitéAWS partagée et](#) le billet de GDPR blog sur le blog sur la AWS sécurité.

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

- Utilisez l'authentification multifactorielle (MFA) pour chaque compte.
- Utilisez SSL/TLS pour communiquer avec les AWS ressources. Nous avons besoin de la TLS version 1.2 et recommandons la TLS version 1.3.
- Configuration API et journalisation de l'activité des utilisateurs avec AWS CloudTrail.
- Utilisez des solutions de AWS chiffrement, ainsi que tous les contrôles de sécurité par défaut qu'ils contiennent 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 FIPS 140 à 3 modules cryptographiques validés pour accéder AWS via une interface de ligne de commande ou unAPI, utilisez un point de terminaison. FIPS Pour plus d'informations sur les FIPS points de terminaison disponibles, voir [Federal Information Processing Standard \(FIPS\) 140-3](#).

Nous vous recommandons fortement de ne jamais placer d'informations confidentielles ou sensibles, telles que les adresses e-mail de vos clients, dans des balises ou des champs de texte libre tels que le champ Name (Nom). Cela inclut lorsque vous travaillez avec CodeStar ou d'autres Services AWS utilisateurs de la consoleAPI, AWS CLI, ou AWS SDKs. Toutes les données que vous entrez dans des balises ou des champs de texte de forme libre utilisés pour les noms peuvent être utilisées à des fins de facturation ou dans les journaux de diagnostic. Si vous fournissez un URL à un serveur externe, nous vous recommandons vivement de ne pas inclure d'informations d'identification dans le URL afin de valider votre demande auprès de ce serveur.

Chiffrement des données dans AWS CodeStar

Par défaut, AWS CodeStar chiffre les informations stockées sur votre projet. Toutes informations autres que votre ID de projet sont chiffrées au repos, comme le nom du projet, la description et les adresses e-mail des utilisateurs. Évitez de mettre des informations personnelles dans votre projetIDs. AWS CodeStar chiffre également les informations en transit par défaut. Aucune action du client n'est requise pour le chiffrement au repos ni le chiffrement en transit.

Identity and Access Management (IAM) pour AWS CodeStar

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. IAMles administrateurs contrôlent qui peut être authentifié (connecté) et autorisé (autorisé) à utiliser les AWS CodeStar ressources. IAMest un Service AWS outil que vous pouvez utiliser sans frais supplémentaires.

Rubriques

- [Public ciblé](#)
- [Authentification avec des identités](#)
- [Gestion des accès à l'aide de politiques](#)
- [Comment AWS CodeStar fonctionne avec IAM](#)

- [AWS CodeStar Politiques et autorisations au niveau du projet](#)
- [AWS CodeStar Exemples de politiques basées sur l'identité](#)
- [Résolution des problèmes d'identité et d'accès liés à AWS CodeStar](#)

Public ciblé

La façon dont vous utilisez AWS Identity and Access Management (IAM) varie en fonction du travail que vous effectuez AWS CodeStar.

Utilisateur du service : si vous utilisez le AWS CodeStar service pour effectuer votre travail, votre administrateur vous fournit les informations d'identification et les autorisations dont vous avez besoin. Au fur et à mesure que vous utilisez de nouvelles AWS CodeStar fonctionnalités 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 pouvez pas accéder à une fonctionnalité dans AWS CodeStar, consultez [Résolution des problèmes d'identité et d'accès liés à AWS CodeStar](#).

Administrateur du service — Si vous êtes responsable des AWS CodeStar ressources de votre entreprise, vous avez probablement un accès complet à AWS CodeStar. C'est à vous de déterminer les AWS CodeStar fonctionnalités et les ressources auxquelles les utilisateurs de votre service doivent accéder. Vous devez ensuite envoyer des demandes à votre IAM administrateur pour modifier les autorisations des utilisateurs de votre service. Consultez les informations de cette page pour comprendre les concepts de base de IAM. Pour en savoir plus sur la façon dont votre entreprise peut utiliser IAM avec AWS CodeStar, voir [Comment AWS CodeStar fonctionne avec IAM](#).

IAM administrateur — Si vous êtes IAM administrateur, vous souhaitez peut-être en savoir plus sur la manière dont vous pouvez rédiger des politiques pour gérer l'accès à AWS CodeStar. Pour consulter des exemples de politiques AWS CodeStar basées sur l'identité que vous pouvez utiliser dans IAM, consultez. [AWS CodeStar Exemples de politiques basées sur l'identité](#)

Authentification avec 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 que Utilisateur racine d'un compte AWS, en tant qu'IAM utilisateur ou en assumant un IAM rôle.

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 en tant qu'identité fédérée, votre administrateur a préalablement configuré la fédération d'identité à l'aide de IAM rôles. Lorsque vous accédez à AWS l'aide de la fédération, vous assumez indirectement un rôle.

Selon le type d'utilisateur que vous êtes, vous pouvez vous connecter au portail AWS Management Console ou au portail AWS d'accès. Pour plus d'informations sur la connexion à AWS, consultez la section [Comment vous connecter à votre compte Compte AWS dans](#) le guide de Connexion à AWS l'utilisateur.

Si vous y accédez AWS par programmation, AWS fournit un kit de développement logiciel (SDK) et une interface de ligne de commande (CLI) pour signer cryptographiquement vos demandes à l'aide de vos informations d'identification. Si vous n'utilisez pas d' AWS outils, vous devez signer vous-même les demandes. Pour plus d'informations sur l'utilisation de la méthode recommandée pour signer vous-même les demandes, consultez la section [Signature des AWS API demandes](#) dans le guide de IAM l'utilisateur.

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, consultez [Authentification multifactorielle](#) dans le guide de AWS IAM Identity Center l'utilisateur et [Utilisation de l'authentification multifactorielle \(MFA\) AWS dans](#) le guide de l'IAMutilisateur.

Compte AWS utilisateur root

Lorsque vous créez un Compte AWS, vous commencez par une identité de connexion unique qui donne un accès complet à toutes Services AWS les ressources du compte. Cette identité est appelée utilisateur Compte AWS root et est accessible en vous connectant avec l'adresse e-mail et le mot de passe que vous avez utilisés pour créer le compte. Il est vivement recommandé de ne pas utiliser l'utilisateur racine pour vos tâches quotidiennes. Protégez vos informations d'identification d'utilisateur racine et utilisez-les pour effectuer les tâches que seul l'utilisateur racine peut effectuer. Pour obtenir la liste complète des tâches qui nécessitent que vous vous connectiez en tant qu'utilisateur root, consultez la section [Tâches nécessitant des informations d'identification utilisateur root](#) dans le guide de IAM l'utilisateur.

IAMutilisateurs et groupes

Un [IAMutilisateur](#) est une identité au sein de vous Compte AWS qui possède des autorisations spécifiques pour une seule personne ou une seule application. Dans la mesure du possible, nous

vous recommandons de vous appuyer sur des informations d'identification temporaires plutôt que de créer des IAM utilisateurs dotés d'informations d'identification à long terme, telles que des mots de passe et des clés d'accès. Toutefois, si vous avez des cas d'utilisation spécifiques qui nécessitent des informations d'identification à long terme auprès des IAM utilisateurs, nous vous recommandons de faire pivoter les clés d'accès. Pour plus d'informations, voir [Rotation régulière des clés d'accès pour les cas d'utilisation nécessitant des informations d'identification à long terme](#) dans le Guide de IAM l'utilisateur.

Un [IAMgroupe](#) est une identité qui définit un ensemble d'IAMutilisateurs. Vous ne pouvez pas vous connecter en tant que groupe. Vous pouvez utiliser les groupes pour spécifier des autorisations pour plusieurs utilisateurs à la fois. Les groupes permettent de gérer plus facilement les autorisations pour de grands ensembles d'utilisateurs. Par exemple, vous pouvez nommer un groupe IAMAdminset lui donner les autorisations nécessaires pour administrer IAM des ressources.

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, voir [Quand créer un IAM utilisateur \(au lieu d'un rôle\)](#) dans le Guide de IAM l'utilisateur.

IAMRôles

Un [IAMrôle](#) est une identité au sein de Compte AWS vous dotée d'autorisations spécifiques. Il est similaire à un IAM utilisateur, mais n'est pas associé à une personne en particulier. Vous pouvez assumer temporairement un IAM rôle dans le en AWS Management Console [changeant de rôle](#). Vous pouvez assumer un rôle en appelant une AWS API opération AWS CLI or ou en utilisant une option personnaliséeURL. Pour plus d'informations sur les méthodes d'utilisation des rôles, consultez la section [Utilisation IAM des rôles](#) dans le Guide de IAM l'utilisateur.

IAMles rôles dotés d'informations d'identification temporaires sont utiles dans les situations suivantes :

- 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 plus d'informations sur les rôles pour la fédération, voir [Création d'un rôle pour un fournisseur d'identité tiers](#) dans le guide de IAM l'utilisateur. Si vous utilisez IAM Identity Center, vous configurez un ensemble d'autorisations. Pour contrôler les accès auxquels vos identités peuvent accéder après leur authentification, IAM Identity Center met en corrélation l'ensemble d'autorisations avec un

rôle dans IAM. Pour plus d'informations sur les jeux d'autorisations, consultez la rubrique [Jeux d'autorisations](#) dans le Guide de l'utilisateur AWS IAM Identity Center .

- **Autorisations IAM utilisateur temporaires** : un IAM utilisateur ou un rôle peut assumer un IAM rôle afin d'obtenir temporairement différentes autorisations pour une tâche spécifique.
- **Accès entre comptes** : vous pouvez utiliser un IAM rôle pour autoriser une personne (un mandant fiable) d'un autre compte à 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 connaître la différence entre les rôles et les politiques basées sur les ressources pour l'accès entre comptes, voir [Accès aux ressources entre comptes IAM dans le guide](#) de l'IAM utilisateur.
- **Accès multiservices** — Certains Services AWS utilisent des fonctionnalités dans d'autres Services AWS. Par exemple, lorsque vous effectuez un appel dans un service, il est courant que ce service exécute des applications dans Amazon EC2 ou stocke des objets dans Amazon S3. Un service peut le faire en utilisant les autorisations d'appel du principal, un rôle de service ou un rôle lié au service.
- **Sessions d'accès transmises (FAS)** — Lorsque vous utilisez un IAM utilisateur ou un rôle pour effectuer des actions AWS, vous êtes considéré comme un mandant. Lorsque vous utilisez certains services, vous pouvez effectuer une action qui initie une autre action dans un autre service. FAS utilise les autorisations du principal appelant au Service AWS, combinées à la demande Service AWS pour adresser des demandes aux services en aval. FAS les demandes 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 les politiques relatives à l'envoi de FAS demandes, consultez la section [Transférer les sessions d'accès](#).
- **Rôle de service** — Un rôle de service est un [IAM rôle](#) qu'un service assume pour effectuer des actions en votre nom. Un IAM administrateur peut créer, modifier et supprimer un rôle de service de l'intérieur IAM. Pour plus d'informations, consultez [la section Création d'un rôle auquel déléguer des autorisations Service AWS](#) dans le Guide de l'utilisateur IAM.
- **Rôle lié à un service** — Un rôle lié à un service est un type de rôle de service lié à un Service AWS. Le service peut endosser le rôle afin d'effectuer une action en votre nom. Les rôles liés à un service apparaissent dans votre Compte AWS répertoire et appartiennent au service. Un IAM administrateur peut consulter, mais pas modifier les autorisations pour les rôles liés à un service.
- **Applications exécutées sur Amazon EC2** : vous pouvez utiliser un IAM rôle pour gérer les informations d'identification temporaires pour les applications qui s'exécutent sur une EC2 instance

et qui font AWS CLI des AWS API demandes. Cela est préférable au stockage des clés d'accès dans l'EC2instance. Pour attribuer un AWS rôle à une EC2 instance et le rendre disponible pour toutes ses applications, vous devez créer un profil d'instance attaché à l'instance. Un profil d'instance contient le rôle et permet aux programmes exécutés sur l'EC2instance d'obtenir des informations d'identification temporaires. Pour plus d'informations, consultez la section [Utilisation d'un IAM rôle pour accorder des autorisations aux applications exécutées sur des EC2 instances Amazon](#) dans le Guide de IAM l'utilisateur.

Pour savoir s'il faut utiliser IAM des rôles ou des IAM utilisateurs, voir [Quand créer un IAM rôle \(au lieu d'un utilisateur\)](#) dans le guide de IAM l'utilisateur.

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 JSON documents. Pour plus d'informations sur la structure et le contenu des documents de JSON politique, voir [Présentation des JSON politiques](#) dans le guide de IAM l'utilisateur.

Les administrateurs peuvent utiliser AWS JSON des politiques 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 autoriser les utilisateurs à effectuer des actions sur les ressources dont ils ont besoin, un IAM administrateur peut créer des IAM politiques. L'administrateur peut ensuite ajouter les IAM politiques aux rôles, et les utilisateurs peuvent assumer les rôles.

IAMles politiques définissent les autorisations pour une action, quelle que soit la méthode que vous utilisez pour effectuer l'opération. Par exemple, supposons que vous disposiez d'une politique qui autorise l'action `iam:GetRole`. Un utilisateur doté de cette politique peut obtenir des informations sur le rôle auprès du AWS Management Console AWS CLI, ou du AWS API.

politiques basées sur l'identité

Les politiques basées sur l'identité sont JSON des documents de politique d'autorisation que vous pouvez joindre à une identité, telle qu'un IAM utilisateur, un groupe d'utilisateurs ou un rôle. Ces politiques contrôlent quel type d'actions des utilisateurs et des rôles peuvent exécuter, sur quelles ressources et dans quelles conditions. Pour savoir comment créer une politique basée sur l'identité, consultez la section [Création de IAM politiques](#) dans le Guide de l'IAMutilisateur.

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 savoir comment choisir entre une politique gérée ou une politique intégrée, voir [Choisir entre des politiques gérées et des politiques intégrées dans le Guide](#) de l'IAMutilisateur.

Politiques basées sur une ressource

Les politiques basées sur les ressources sont des documents JSON de stratégie que vous attachez à une ressource. Les politiques de confiance dans les IAM rôles et les politiques relatives aux compartiments Amazon S3 sont des exemples de politiques basées sur les ressources. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour contrôler l'accès à une ressource spécifique. Pour la ressource dans laquelle se trouve la politique, cette dernière définit quel type d'actions un principal spécifié peut effectuer sur cette ressource et dans quelles conditions. Vous devez [spécifier un principal](#) dans une politique basée sur les ressources. Les principaux peuvent inclure des comptes, des utilisateurs, des rôles, des utilisateurs fédérés ou. Services AWS

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

Listes de contrôle d'accès (ACLs)

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

Amazon S3 et Amazon VPC sont des exemples de services compatibles ACLs. AWS WAF Pour en savoir plus ACLs, consultez la [présentation de la liste de contrôle d'accès \(ACL\)](#) dans le guide du développeur Amazon Simple Storage Service.

Autres types de politique

AWS prend en charge d'autres types de politiques moins courants. Ces types de politiques peuvent définir le nombre maximum d'autorisations qui vous sont accordées par des types de politiques plus courants.

- **Limites d'autorisations** — Une limite d'autorisations est une fonctionnalité avancée dans laquelle vous définissez le maximum d'autorisations qu'une politique basée sur l'identité peut accorder à une IAM entité (IAMutilisateur ou rôle). Vous pouvez définir une limite d'autorisations pour une entité. Les autorisations en résultant représentent la combinaison des politiques basées sur l'identité d'une entité et de ses limites d'autorisation. Les politiques basées sur les ressources qui spécifient l'utilisateur ou le rôle dans le champ `Principal` ne sont pas limitées par les limites d'autorisations. Un refus explicite dans l'une de ces politiques remplace l'autorisation. Pour plus d'informations sur les limites d'autorisations, consultez la section [Limites d'autorisations pour les IAM entités](#) dans le Guide de IAM l'utilisateur.
- **Politiques de contrôle des services (SCPs)** : SCPs JSON politiques qui spécifient les autorisations maximales pour une organisation ou une unité organisationnelle (UO) dans AWS Organizations. AWS Organizations est un service permettant de regrouper et de gérer de manière centralisée Comptes AWS les multiples propriétés de votre entreprise. Si vous activez toutes les fonctionnalités d'une organisation, vous pouvez appliquer des politiques de contrôle des services (SCPs) à l'un ou à l'ensemble de vos comptes. Les SCP limites d'autorisations pour les entités présentes dans les comptes des membres, y compris chacune d'entre elles Utilisateur racine d'un compte AWS. Pour plus d'informations sur les Organizations et consultez SCPs les [politiques de contrôle des services](#) dans le Guide de AWS Organizations l'utilisateur.
- **Politiques de séance** : les politiques de séance sont des politiques avancées que vous utilisez en tant que paramètre lorsque vous créez par programmation une séance temporaire pour un rôle ou un utilisateur fédéré. Les autorisations de séance en résultant sont une combinaison des politiques basées sur l'identité de l'utilisateur ou du rôle et des politiques de séance. Les autorisations peuvent également provenir d'une politique basée sur les ressources. Un refus explicite dans l'une de ces politiques annule l'autorisation. Pour plus d'informations, consultez la section [Politiques de session](#) dans le guide de IAM l'utilisateur.

Types de politique multiple

Lorsque plusieurs types de politiques s'appliquent à la requête, les autorisations en résultant sont plus compliquées à comprendre. Pour savoir comment AWS déterminer s'il faut autoriser

une demande lorsque plusieurs types de politiques sont impliqués, consultez la section [Logique d'évaluation des politiques](#) dans le guide de IAM l'utilisateur.

Comment AWS CodeStar fonctionne avec IAM

Avant IAM de gérer l'accès à AWS CodeStar, vous devez connaître les IAM fonctionnalités disponibles AWS CodeStar. Pour obtenir une vue d'ensemble du mode de fonctionnement des autres AWS services AWS CodeStar et des autres services IAM, consultez la section [AWS Services compatibles IAM](#) dans le guide de IAM l'utilisateur.

Rubriques

- [AWS CodeStar Politiques basées sur l'identité](#)
- [AWS CodeStar Politiques basées sur les ressources](#)
- [Autorisation basée sur les balises AWS CodeStar](#)
- [AWS CodeStar IAM Rôles](#)
- [IAM Accès utilisateur à AWS CodeStar](#)
- [Accès utilisateur fédéré à AWS CodeStar](#)
- [Utilisation d'informations d'identification temporaires avec AWS CodeStar](#)
- [Rôles liés à un service](#)
- [Rôles de service](#)

AWS CodeStar Politiques basées sur l'identité

Avec IAM les politiques basées sur l'identité, vous pouvez spécifier les actions et les ressources autorisées ou refusées, ainsi que les conditions dans lesquelles les actions sont autorisées ou refusées. AWS CodeStar crée plusieurs politiques basées sur l'identité en votre nom, qui permettent de AWS CodeStar créer et de gérer des ressources dans le cadre d'un AWS CodeStar projet. AWS CodeStar prend 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 JSON politique, consultez la section [Référence des éléments de IAM JSON stratégie](#) dans le guide de IAM l'utilisateur.

Actions

Les administrateurs peuvent utiliser AWS JSON des politiques 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 d'une JSON politique décrit les actions que vous pouvez utiliser pour autoriser ou refuser l'accès dans une politique. Les actions de stratégie portent généralement le même nom que l'opération associée. Il existe certaines exceptions, telles que les actions avec autorisation uniquement qui n'ont pas d'opération correspondante. API 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 politique en AWS CodeStar cours utilisent le préfixe suivant avant l'action :`codestar:`. Par exemple, pour autoriser un IAM utilisateur spécifique à modifier les attributs d'un AWS CodeStar projet, tels que sa description, vous pouvez utiliser la déclaration de politique suivante :

```
{
  "Version": "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "codestar:UpdateProject"
      ],
      "Resource" : "arn:aws:codestar:us-east-2:project/my-first-projec"
    }
  ]
}
```

Les déclarations de politique doivent inclure un élément `Action` ou `NotAction`. AWS CodeStar définit son propre ensemble d'actions décrivant les tâches que vous pouvez effectuer avec ce service.

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

```
"Action": [
  "codestar:action1",
  "codestar:action2"
```

Vous pouvez aussi spécifier 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:List*"
```

Pour consulter la liste des AWS CodeStar actions, reportez-vous à la section [Actions définies par AWS CodeStar](#) dans le guide de IAM l'utilisateur.

Ressources

Les administrateurs peuvent utiliser AWS JSON des politiques 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 Resource JSON de stratégie indique le ou les objets auxquels s'applique l'action. Les instructions doivent inclure un élément Resource ou NotResource. Il est recommandé de spécifier une ressource en utilisant son [Amazon Resource Name \(ARN\)](#). Vous pouvez le faire pour des actions qui prennent en charge un type de ressource spécifique, connu sous la dénomination autorisations de niveau ressource.

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

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

La ressource AWS CodeStar du projet comprend les éléments suivants ARN :

```
arn:aws:codestar:region:account:project/resource-specifier
```

Pour plus d'informations sur le format de ARNs, consultez [Amazon Resource Names \(ARNs\) et AWS Service Namespaces](#).

Par exemple, ce qui suit indique le nom AWS CodeStar du projet *my-first-projec* enregistré sur le AWS compte 111111111111 dans la AWS région us-east-2 :

```
arn:aws:codestar:us-east-2:111111111111:project/my-first-projec
```

Ce qui suit indique tout AWS CodeStar projet qui commence par le nom *my-proj* enregistré sur le AWS compte 111111111111 dans la AWS région us-east-2 :

```
arn:aws:codestar:us-east-2:111111111111:project/my-proj*
```

Certaines AWS CodeStar actions, par exemple pour répertorier des projets, ne peuvent pas être effectuées sur une ressource. Dans ces cas-là, vous devez utiliser le caractère générique (*).

```
"LisProjects": "*"
```

Pour consulter la liste des types de AWS CodeStar ressources et leurs caractéristiquesARNs, reportez-vous à la section [Ressources définies par AWS CodeStar](#) dans le guide de IAM l'utilisateur. Pour savoir avec quelles actions vous pouvez spécifier pour chaque ressource, consultez la ARN section [Actions définies par AWS CodeStar](#).

Clés de condition

AWS CodeStar ne fournit aucune clé de condition spécifique au service, mais il prend en charge l'utilisation de certaines clés de condition globales. Pour voir toutes les clés de condition AWS globales, voir [Clés contextuelles de condition AWS globale](#) dans le guide de IAM l'utilisateur.

Exemples

Pour consulter des exemples de politiques AWS CodeStar basées sur l'identité, consultez. [AWS CodeStarExemples de politiques basées sur l'identité](#)

AWS CodeStar Politiques basées sur les ressources

AWS CodeStar ne prend pas en charge les politiques basées sur les ressources.

Autorisation basée sur les balises AWS CodeStar

Vous pouvez associer des balises à AWS CodeStar des projets ou transmettre des balises dans une demande adressée à AWS CodeStar. 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:ResourceTag/key-name`, `aws:RequestTag/key-name` ou `aws:TagKeys`. Pour plus d'informations sur le balisage AWS CodeStar des ressources, consultez [the section called "Utilisation des balises de projet"](#).

Pour consulter un exemple de politique basée sur l'identité permettant de limiter l'accès à un AWS CodeStar projet en fonction des balises associées à ce projet, voir. [Affichage des projets AWS CodeStar en fonction des balises](#)

AWS CodeStar IAM Rôles

Un [IAM rôle](#) est une entité de votre AWS compte dotée d'autorisations spécifiques.

Vous pouvez l'utiliser AWS CodeStar en tant qu'[IAM utilisateur](#), utilisateur fédéré, utilisateur root ou en tant que rôle assumé. Tous les types d'utilisateurs disposant des autorisations appropriées peuvent gérer les autorisations de projet relatives à leurs AWS ressources, mais AWS CodeStar les autorisations de projet sont gérées automatiquement pour IAM les utilisateurs. [IAM les politiques](#) et [les rôles](#) accordent des autorisations et un accès à cet utilisateur en fonction du rôle du projet. Vous pouvez utiliser la IAM console pour créer d'autres politiques qui AWS CodeStar attribuent d'autres autorisations à un IAM utilisateur.

Par exemple, vous voudrez peut-être autoriser un utilisateur à afficher un projet AWS CodeStar, mais pas à le modifier. Dans ce cas, vous ajoutez l'IAM utilisateur à un AWS CodeStar projet avec le rôle d'observateur. Chaque AWS CodeStar projet possède un ensemble de règles qui vous aident à contrôler l'accès au projet. En outre, vous pouvez contrôler les utilisateurs auxquels ils ont accès AWS CodeStar.

AWS CodeStar l'accès est géré différemment pour les IAM utilisateurs et pour les utilisateurs fédérés. Seuls IAM les utilisateurs peuvent être ajoutés aux équipes. Pour accorder IAM aux utilisateurs des autorisations sur les projets, vous ajoutez l'utilisateur à l'équipe du projet et vous lui attribuez un rôle. Pour accorder aux utilisateurs fédérés des autorisations sur les projets, vous devez associer manuellement la politique gérée du rôle du AWS CodeStar projet au rôle de l'utilisateur fédéré.

Ce tableau récapitule les outils disponibles pour chaque type d'accès.

Fonction des autorisations	IAM utilisateur	Utilisateur fédéré	Utilisateur root
SSH gestion des clés pour l'accès à distance pour les projets Amazon EC2 et Elastic Beanstalk	✓		
AWS CodeCommit SSH accès	✓		
IAM autorisations utilisateur gérées par AWS CodeStar	✓		
Autorisations de projet gérées manuellement		✓	✓

Fonction des autorisations	IAMutilisateur	Utilisateur fédéré	Utilisateur root
Les utilisateurs peuvent être ajoutés à un projet en tant que membres d'équipe	✓		

IAMAccès utilisateur à AWS CodeStar

Lorsque vous ajoutez un IAM utilisateur à un projet et que vous choisissez un rôle pour cet utilisateur, AWS CodeStar applique automatiquement la politique appropriée à l'IAMutilisateur. Pour IAM les utilisateurs, il n'est pas nécessaire de joindre ou de gérer directement des politiques ou des autorisationsIAM. Pour plus d'informations sur l'ajout IAM d'un utilisateur à un AWS CodeStar projet, consultez [Ajouter des membres de l'équipe à un projet AWS CodeStar](#). Pour plus d'informations sur la suppression IAM d'un utilisateur d'un AWS CodeStar projet, consultez [Supprimer des membres d'une équipe dans un projet AWS CodeStar](#).

Associer une politique intégrée à un utilisateur IAM

Lorsque vous ajoutez un utilisateur à un projet, la politique gérée correspondant au rôle de l'utilisateur est AWS CodeStar automatiquement attachée au projet. Vous ne devez pas associer manuellement une politique AWS CodeStar gérée pour un projet à un IAM utilisateur. À l'exception de `AWSCodeStarFullAccess`, nous vous déconseillons de joindre des politiques qui modifient les autorisations IAM d'un utilisateur dans un AWS CodeStar projet. Si vous décidez de créer et d'associer vos propres politiques, consultez la section [Ajouter et supprimer des autorisations IAM d'identité](#) dans le guide de IAM l'utilisateur.

Accès utilisateur fédéré à AWS CodeStar

Au lieu de créer un IAM utilisateur ou d'utiliser l'utilisateur root, vous pouvez utiliser des identités utilisateur provenant de AWS Directory Service votre annuaire d'entreprise, d'un fournisseur d'identité Web ou d'IAMutilisateurs assumant des rôles. Ces derniers sont appelés utilisateurs fédérés.

Accordez aux utilisateurs fédérés l'accès à votre AWS CodeStar projet en associant manuellement les politiques gérées décrites dans [Politiques et autorisations AWS CodeStar au niveau du projet au rôle](#) de l'utilisateur. IAM Vous associez la politique du propriétaire, du contributeur ou du spectateur après avoir AWS CodeStar créé les ressources et les IAM rôles de votre projet.

Prérequis :

- Vous devez avoir configuré un fournisseur d'identité. Par exemple, vous pouvez configurer un fournisseur d'identité SAML et configurer l'AWS authentication par le biais de ce fournisseur. Pour plus d'informations sur la configuration d'un fournisseur d'identité, consultez la section [Création de fournisseurs IAM d'identité](#). Pour plus d'informations sur SAML la fédération, voir À [propos de la fédération SAML basée sur la version 2.0](#).
- Vous devez avoir créé un rôle que doit assumer un utilisateur fédéré lorsqu'un accès est demandé par l'intermédiaire d'un [fournisseur d'identité](#). Une politique de STS confiance doit être attachée au rôle afin de permettre aux utilisateurs fédérés d'assumer ce rôle. Pour plus d'informations, consultez la section [Utilisateurs et rôles fédérés](#) dans le guide de l'IAM utilisateur.
- Vous devez avoir créé votre AWS CodeStar projet et en connaître l'identifiant.

Pour plus d'informations sur la création d'un rôle pour les fournisseurs d'identité, consultez [Création d'un rôle pour un fournisseur d'identité tiers \(Fédération\)](#).

Associer la politique `AWSCodeStarFullAccess` gérée au rôle de l'utilisateur fédéré

Accordez à un utilisateur fédéré les autorisations nécessaires pour créer un projet en attachant la stratégie gérée `AWSCodeStarFullAccess`. Pour effectuer ces étapes, vous devez vous être connecté à la console soit en tant qu'utilisateur root, soit en tant qu'utilisateur administrateur du compte, soit en tant qu'IAM utilisateur ou utilisateur fédéré doté de la politique `AdministratorAccess` gérée associée ou d'un équivalent.

Note

Une fois que vous avez créé le projet, vos autorisations de propriétaire du projet ne sont pas appliquées automatiquement. En utilisant un rôle disposant d'autorisations administratives pour votre compte, attachez la stratégie gérée de propriétaire, comme décrit dans [Associez la politique gérée par le AWS CodeStar visualiseur/contributeur/propriétaire de votre projet au rôle de l'utilisateur fédéré](#).

1. Ouvrez la IAM console. Dans le panneau de navigation, choisissez Politiques.
2. Entrez `AWSCodeStarFullAccess` dans le champ de recherche. Le nom de la stratégie s'affiche, avec le type de politique AWS gérée. Vous pouvez développer la stratégie pour voir les autorisations qui figurent dans sa déclaration.
3. Sélectionnez le cercle en regard de la stratégie puis, sous Actions de stratégie, choisissez Attacher.

4. Sur la page Récapitulatif, choisissez l'onglet Entités attachées. Choisissez Attacher.
5. Sur la page Attacher la stratégie, filtrez sur le rôle de l'utilisateur fédéré dans le champ de recherche. Cochez la case en regard du nom du rôle, puis choisissez Attacher la stratégie. L'onglet Entités attachées affiche le nouvel attachement.

Associez la politique gérée par le AWS CodeStar visualiseur/contributeur/propriétaire de votre projet au rôle de l'utilisateur fédéré

Accordez aux utilisateurs fédérés l'accès à votre projet en attachant la stratégie de propriétaire, de participant ou de lecteur au rôle de l'utilisateur. La stratégie gérée accorde le niveau d'autorisations approprié. Contrairement aux IAM utilisateurs, vous devez associer et détacher manuellement les politiques gérées pour les utilisateurs fédérés. Cela revient à attribuer des autorisations de projet aux membres de l'équipe dans AWS CodeStar. Pour effectuer ces étapes, vous devez vous être connecté à la console soit en tant qu'utilisateur root, soit en tant qu'utilisateur administrateur du compte, soit en tant qu'IAM utilisateur ou utilisateur fédéré doté de la politique AdministratorAccess gérée associée ou d'un équivalent.

Prérequis :

- Vous devez avoir créé un rôle ou disposer d'un rôle existant qu'assume votre utilisateur fédéré.
- Vous devez savoir quel niveau d'autorisations accorder. Les stratégies gérées attachées aux rôles de propriétaire, de participant et de lecteur confèrent des autorisations basées sur le rôle pour votre projet.
- Votre AWS CodeStar projet doit avoir été créé. La politique gérée n'est pas disponible IAM tant que le projet n'est pas créé.

1. Ouvrez la IAM console. Dans le panneau de navigation, choisissez Politiques.
2. Entrez l'ID de votre projet dans le champ de recherche. Le nom de la stratégie correspondant à votre projet s'affiche avec le type de stratégie Stratégies gérées par le client. Vous pouvez développer la stratégie pour voir les autorisations qui figurent dans sa déclaration.
3. Choisissez l'une de ces stratégies gérées. Sélectionnez le cercle en regard de la stratégie puis, sous Actions de stratégie, choisissez Attacher.
4. Sur la page Récapitulatif, choisissez l'onglet Entités attachées. Choisissez Attacher.
5. Sur la page Attacher la stratégie, filtrez sur le rôle de l'utilisateur fédéré dans le champ de recherche. Cochez la case en regard du nom du rôle, puis choisissez Attacher la stratégie. L'onglet Entités attachées affiche le nouvel attachement.

Détacher une politique AWS CodeStar gérée du rôle de l'utilisateur fédéré

Avant de supprimer votre AWS CodeStar projet, vous devez détacher manuellement toutes les politiques gérées que vous avez associées au rôle d'un utilisateur fédéré. Pour effectuer ces étapes, vous devez vous être connecté à la console soit en tant qu'utilisateur root, soit en tant qu'utilisateur administrateur du compte, soit en tant qu'IAMutilisateur ou utilisateur fédéré doté de la politique AdministratorAccess gérée associée ou d'un équivalent.

1. Ouvrez la IAM console. Dans le panneau de navigation, choisissez Politiques.
2. Entrez l'ID de votre projet dans le champ de recherche.
3. Sélectionnez le cercle en regard de la stratégie puis, sous Actions de stratégie, choisissez Attacher.
4. Sur la page Récapitulatif, choisissez l'onglet Entités attachées.
5. Dans le champ de recherche, filtrez sur le rôle de l'utilisateur fédéré. Choisissez Détacher.

Associer une politique AWS Cloud9 gérée au rôle de l'utilisateur fédéré

Si vous utilisez un environnement de AWS Cloud9 développement, accordez aux utilisateurs fédérés l'accès à celui-ci en associant la politique AWSCloud9User gérée au rôle de l'utilisateur. Contrairement aux IAM utilisateurs, vous devez associer et détacher manuellement les politiques gérées pour les utilisateurs fédérés. Pour effectuer ces étapes, vous devez vous être connecté à la console soit en tant qu'utilisateur root, soit en tant qu'utilisateur administrateur du compte, soit en tant qu'IAMutilisateur ou utilisateur fédéré doté de la politique AdministratorAccess gérée associée ou d'un équivalent.

Prérequis :

- Vous devez avoir créé un rôle ou disposer d'un rôle existant qu'assume votre utilisateur fédéré.
- Vous devez savoir quel niveau d'autorisations accorder :
 - La stratégie gérée AWSCloud9User permet à l'utilisateur d'effectuer les opérations suivantes :
 - Créez leurs propres environnements AWS Cloud9 de développement.
 - Obtenir des informations sur son environnement
 - Modifier les paramètres de son environnement
 - La stratégie gérée AWSCloud9Administrator permet à l'utilisateur d'effectuer les opérations suivantes pour lui-même ou pour d'autres utilisateurs :
 - Créer des environnements

- Obtenir des informations sur les environnements
 - Supprimer des environnements
 - Modifier les paramètres d'environnements
1. Ouvrez la IAM console. Dans le panneau de navigation, choisissez Politiques.
 2. Entrez le nom de la stratégie dans le champ de recherche. La stratégie gérée s'affiche, avec le type de stratégie AWS gérée. Vous pouvez développer la stratégie pour voir les autorisations qui figurent dans sa déclaration.
 3. Choisissez l'une de ces stratégies gérées. Sélectionnez le cercle en regard de la stratégie puis, sous Actions de stratégie, choisissez Attacher.
 4. Sur la page Récapitulatif, choisissez l'onglet Entités attachées. Choisissez Attacher.
 5. Sur la page Attacher la stratégie, filtrez sur le rôle de l'utilisateur fédéré dans le champ de recherche. Cochez la case en regard du nom du rôle, puis choisissez Attacher la stratégie. L'onglet Entités attachées affiche le nouvel attachement.

Détacher une politique AWS Cloud9 gérée du rôle de l'utilisateur fédéré

Si vous utilisez un environnement de AWS Cloud9 développement, vous pouvez supprimer l'accès d'un utilisateur fédéré à celui-ci en détachant la politique qui accorde l'accès. Pour effectuer ces étapes, vous devez vous être connecté à la console soit en tant qu'utilisateur root, soit en tant qu'utilisateur administrateur du compte, soit en tant qu'IAMutilisateur ou utilisateur fédéré doté de la politique AdministratorAccess gérée associée ou d'un équivalent.

1. Ouvrez la IAM console. Dans le panneau de navigation, choisissez Politiques.
2. Entrez le nom de votre projet dans le champ de recherche.
3. Sélectionnez le cercle en regard de la stratégie puis, sous Actions de stratégie, choisissez Attacher.
4. Sur la page Récapitulatif, choisissez l'onglet Entités attachées.
5. Dans le champ de recherche, filtrez sur le rôle de l'utilisateur fédéré. Choisissez Détacher.

Utilisation d'informations d'identification temporaires avec AWS CodeStar

Vous pouvez utiliser des informations d'identification temporaires pour vous connecter à la fédération, assumer un IAM rôle ou assumer un rôle entre comptes. Vous obtenez des informations

d'identification de sécurité temporaires en appelant AWS STS API des opérations telles que [AssumeRole](#) ou [GetFederationToken](#).

AWS CodeStar prend en charge l'utilisation d'informations d'identification temporaires, mais la fonctionnalité réservée aux membres de l' AWS CodeStar équipe ne fonctionne pas pour l'accès fédéré. AWS CodeStar la fonctionnalité des membres de l'équipe prend uniquement en charge l'ajout IAM d'un utilisateur en tant que membre de l'équipe.

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 au service apparaissent dans votre IAM compte et appartiennent au service. Un administrateur peut consulter mais ne peut pas modifier les autorisations concernant les rôles liés à un service.

AWS CodeStar ne prend pas en charge les rôles liés à un service.

Rôles de service

Cette fonction permet à un service d'endosser une [fonction du service](#) en votre nom. Ce rôle autorise le service à accéder à des ressources d'autres services pour effectuer une action en votre nom. Les rôles de service apparaissent dans votre IAM compte et sont détenus par le compte. Cela signifie qu'un administrateur peut modifier les autorisations associées à ce rôle. Toutefois, une telle action peut perturber le bon fonctionnement du service.

AWS CodeStar prend en charge les rôles de service. AWS CodeStar utilise un rôle de service lorsqu'il crée et gère les ressources de votre projet. `aws-codestar-service-role` Pour plus d'informations, consultez la section [Termes et concepts relatifs aux rôles](#) dans le guide de IAM l'utilisateur.

Important

Vous devez être connecté en tant qu'utilisateur administratif ou avec le compte racine pour créer ce rôle de service. Pour plus d'informations, voir [Premier accès uniquement : vos informations d'identification d'utilisateur root](#) et [Création de votre premier utilisateur et groupe d'administrateurs](#) dans le guide de l'IAM utilisateur.

Ce rôle est créé pour vous la première fois que vous créez un projet dans AWS CodeStar. Le rôle de service agit en votre nom pour :

- créer les ressources que vous choisissez lors de la création d'un projet ;
- Affichez les informations relatives à ces ressources dans le tableau de bord AWS CodeStar du projet.

Il agit également en votre nom lorsque vous gérez les ressources d'un projet. Pour obtenir un exemple de cette déclaration de stratégie, veuillez consulter [AWSCodeStarServiceRole Politique](#).

En outre, AWS CodeStar crée plusieurs rôles de service spécifiques au projet, en fonction du type de projet. AWS CloudFormation et des rôles de chaîne d'outils sont créés pour chaque type de projet.

- AWS CloudFormation les rôles permettent AWS CodeStar d'accéder AWS CloudFormation à des piles pour créer et modifier des piles pour votre AWS CodeStar projet.
- Les rôles de la chaîne d'outils permettent d'accéder AWS CodeStar à d'autres AWS services pour créer et modifier des ressources pour votre AWS CodeStar projet.

AWS CodeStar Politiques et autorisations au niveau du projet

Lorsque vous créez un projet, vous AWS CodeStar créez les IAM rôles et les politiques dont vous avez besoin pour gérer les ressources de votre projet. Les stratégies se divisent en trois catégories :

- IAMpolitiques pour les membres de l'équipe de projet.
- IAMpolitiques relatives aux rôles des travailleurs.
- IAMpolitiques pour un rôle d'exécution au moment de l'exécution.

IAMPolitiques pour les membres de l'équipe

Lorsque vous créez un projet, vous AWS CodeStar créez trois politiques gérées par le client pour l'accès du propriétaire, du contributeur et du spectateur au projet. Tous les AWS CodeStar projets contiennent des IAM politiques pour ces trois niveaux d'accès. Ces niveaux d'accès sont spécifiques au projet et définis par une politique IAM gérée portant un nom standard, où *project-id* est l'ID du AWS CodeStar projet (par exemple, *my-first-projec*):

- CodeStar_*project-id*_Owner
- CodeStar_*project-id*_Contributor
- CodeStar_*project-id*_Viewer

⚠ Important

Ces politiques sont susceptibles d'être modifiées par AWS CodeStar. Elles ne doivent pas être modifiées manuellement. Si vous souhaitez ajouter ou modifier des autorisations, associez des politiques supplémentaires à l'IAMutilisateur.

Lorsque vous ajoutez des membres de l'équipe (IAMutilisateurs) au projet et que vous choisissez leurs niveaux d'accès, la politique correspondante est attachée à IAM l'utilisateur, lui octroyant les autorisations appropriées pour agir sur les ressources du projet. Dans la plupart des cas, il n'est pas nécessaire de joindre ou de gérer directement des politiques ou des autorisationsIAM. Il n'est pas recommandé d'associer manuellement une politique de niveau d' AWS CodeStar accès à un IAM utilisateur. Si cela est absolument nécessaire, en complément d'une politique de niveau d' AWS CodeStar accès, vous pouvez créer vos propres politiques gérées ou intégrées pour appliquer votre propre niveau d'autorisations à un IAM utilisateur.

Les stratégies sont étroitement attribuées à des ressources de projet et des actions spécifiques. Au fur et à mesure que de nouvelles ressources sont ajoutées à l'infrastructure, AWS CodeStar tente de mettre à jour les politiques des membres de l'équipe afin d'inclure les autorisations d'accès à la nouvelle ressource, s'il s'agit de l'un des types de ressources pris en charge.

📘 Note

Les politiques relatives aux niveaux d'accès dans un AWS CodeStar projet s'appliquent uniquement à ce projet. Cela permet de garantir que les utilisateurs peuvent uniquement voir et interagir avec les AWS CodeStar projets pour lesquels ils sont autorisés, au niveau déterminé par leur rôle. Seuls les utilisateurs qui créent AWS CodeStar des projets doivent se voir appliquer une politique autorisant l'accès à toutes les AWS CodeStar ressources, quel que soit le projet.

Toutes les politiques relatives AWS CodeStar aux niveaux d'accès varient en fonction des AWS ressources associées au projet auquel les niveaux d'accès sont associés. Contrairement à d'autres services AWS , ces stratégies sont personnalisées lorsque le projet est créé et mises à jour à mesure que les ressources du projet évoluent. Par conséquent, il n'existe pas de stratégie unique et canonique gérée par le propriétaire, le participant ou le lecteur.

AWS CodeStar Politique relative au rôle du propriétaire

La politique gérée par le CodeStar_*project-id*_Owner client permet à un utilisateur d'effectuer toutes les actions du AWS CodeStar projet sans aucune restriction. Il s'agit de la seule stratégie qui permet à un utilisateur d'ajouter ou de supprimer des membres de l'équipe. Le contenu de la stratégie varie selon les ressources associées au projet. Veuillez consulter [AWS CodeStar Politique relative au rôle du propriétaire](#) pour obtenir un exemple.

Un IAM utilisateur doté de cette politique peut effectuer toutes les AWS CodeStar actions du projet, mais contrairement à un IAM utilisateur doté de cette AWSCodeStarFullAccess politique, il ne peut pas créer de projets. L'étendue de l'codestar:*autorisation est limitée à une ressource spécifique (le AWS CodeStar projet associé à cet ID de projet).

AWS CodeStar Politique relative aux rôles des contributeurs

La stratégie CodeStar_*project-id*_Contributor gérée par le client permet à un utilisateur de participer au projet et d'en modifier le tableau de bord, mais elle ne l'autorise pas à ajouter ou à supprimer des membres de l'équipe. Le contenu de la stratégie varie selon les ressources associées au projet. Veuillez consulter [Stratégie de rôle gérée par le participant AWS CodeStar](#) pour obtenir un exemple.

AWS CodeStar Politique relative au rôle du spectateur

La stratégie CodeStar_*project-id*_Viewer gérée par le client permet à un utilisateur d'afficher un projet dans AWS CodeStar, mais pas d'en modifier les ressources ni d'ajouter ou supprimer des membres de l'équipe. Le contenu de la stratégie varie selon les ressources associées au projet. Veuillez consulter [AWS CodeStar Politique relative au rôle du spectateur](#) pour obtenir un exemple.

IAMPolitiques relatives aux rôles des travailleurs

Si vous créez votre AWS CodeStar projet après le 6 décembre 2018PDT, il AWS CodeStar crée deux rôles de travailleur, CodeStar-*project-id*-ToolChain et CodeStar-*project-id*-CloudFormation. Un rôle de travailleur est un IAM rôle spécifique au projet qui AWS CodeStar crée pour passer à un service. Il accorde des autorisations afin que le service puisse créer des ressources et exécuter des actions dans le contexte de votre AWS CodeStar projet. Le rôle de travailleur de la chaîne d'outils entretient une relation de confiance établie avec les services de la chaîne d'outils tels que CodeBuild CodeDeploy, et. CodePipeline Les membres de l'équipe de projet (propriétaires et participants) bénéficient d'un accès pour transmettre le rôle de travail à des services en aval de confiance. Pour voir un exemple de déclaration de stratégie en ligne pour ce rôle, consultez

[AWS CodeStar Politique relative au rôle des travailleurs de la chaîne d'outils \(après le 6 décembre 2018PDT\).](#)

Le rôle de CloudFormation travailleur inclut les autorisations pour certaines ressources prises en charge par AWS CloudFormation, ainsi que les autorisations permettant de créer des IAM utilisateurs, des rôles et des politiques dans votre pile d'applications. Il a également établi une relation de confiance avec AWS CloudFormation. Pour atténuer les risques d'augmentation des privilèges et d'actions destructrices, la politique des AWS CloudFormation rôles inclut une condition qui exige la limite d'autorisations spécifique au projet pour chaque IAM entité (utilisateur ou rôle) créée dans la pile d'infrastructure. Pour voir un exemple de déclaration de stratégie en ligne pour ce rôle, consultez [AWS CloudFormation Politique relative au rôle des travailleurs](#).

Pour les AWS CodeStar projets créés avant le 6 décembre 2018, PDT AWS CodeStar crée des rôles de travail individuels pour les ressources de la chaîne d'outils telles que CodePipeline CodeBuild, et CloudWatch des événements, et crée également un rôle de travailleur pour AWS CloudFormation lequel un ensemble limité de ressources est pris en charge. Chacun de ces rôles dispose d'une relation d'approbation établie avec le service correspondant. Les membres de l'équipe de projet (propriétaires et participants) et certains autres rôles de travail bénéficient d'un accès pour transmettre le rôle de travail à des services en aval de confiance. Les autorisations pour les rôles de travail sont définis dans une stratégie en ligne associée à un ensemble basique d'actions que le rôle peut effectuer sur un ensemble de ressources de projet. Ces autorisations sont statiques. Elles comprennent des autorisations pour des ressources qui sont incluses dans le projet lors de sa création, mais ne sont pas mises à jour lorsque de nouvelles ressources sont ajoutées au projet. Pour des exemples de ces déclarations de stratégies, consultez :

- [AWS CloudFormation Politique relative au rôle des travailleurs \(avant le 6 décembre 2018PDT\)](#)
- [AWS CodePipeline Politique relative au rôle des travailleurs \(avant le 6 décembre 2018PDT\)](#)
- [AWS CodeBuild Politique relative au rôle des travailleurs \(avant le 6 décembre 2018PDT\)](#)
- [Politique relative CloudWatch aux rôles des employés d'Amazon Events \(avant le 6 décembre 2018PDT\)](#)

IAMPolitique relative au rôle d'exécution

Pour les projets créés après le 6 décembre 2018PDT, AWS CodeStar crée un rôle d'exécution générique pour l'exemple de projet dans votre pile d'applications. Ce rôle est limité aux ressources de projet employant la stratégie de limite d'autorisations. Au fur et à mesure que vous développez l'exemple de projet, vous pouvez créer IAM des rôles supplémentaires, et la politique des AWS

CloudFormation rôles exige que ces rôles soient délimités à l'aide de la limite d'autorisation afin d'éviter une escalade des privilèges. Pour de plus amples informations, veuillez consulter [Ajoutez un rôle IAM à un projet](#).

Pour les projets Lambda créés avant le 6 décembre 2018PDT, AWS CodeStar crée un rôle d'exécution Lambda associé à une politique intégrée avec des autorisations permettant d'agir sur les ressources de la pile de projets. AWS SAM Au fur et à mesure que de nouvelles ressources sont ajoutées au SAM modèle, AWS CodeStar tente de mettre à jour la politique de rôle d'exécution Lambda afin d'inclure les autorisations d'accès à la nouvelle ressource s'il s'agit de l'un des types de ressources pris en charge.

Limite d'autorisations IAM

Après le 6 décembre 2018PDT, lorsque vous créez un projet, vous AWS CodeStar créez une politique gérée par le client et attribuez cette politique comme [limite d'IAM autorisation](#) aux IAM rôles du projet. AWS CodeStar exige que toutes les IAM entités créées dans la pile d'applications aient une limite d'autorisations. Une limite des autorisations contrôle les autorisations maximales du rôle, mais ne fournit pas d'autorisations au rôle. Les stratégies d'autorisations définissent les autorisations pour le rôle. Cela signifie que, quel que soit le nombre d'autorisations supplémentaires ajoutées à un rôle, quiconque utilise le rôle ne peut pas exécuter plus que les actions incluses dans la limite d'autorisation. Pour plus d'informations sur la manière dont les politiques d'autorisations et les limites d'autorisations sont évaluées, consultez la section [Logique d'évaluation des politiques](#) dans le guide de IAM l'utilisateur.

AWS CodeStar utilise une limite d'autorisation spécifique au projet pour empêcher l'extension des privilèges à des ressources extérieures au projet. La limite AWS CodeStar des autorisations inclut ARNs les ressources du projet. Pour obtenir un exemple de cette déclaration de stratégie, veuillez consulter [AWS CodeStar Politique relative aux limites des autorisations](#).

La AWS CodeStar transformation met à jour cette politique lorsque vous ajoutez ou supprimez une ressource prise en charge dans le projet par le biais de l'application stack (`template.yml`).

Ajouter une limite d'IAM autorisations aux projets existants

Si votre AWS CodeStar projet a été créé avant le 6 décembre 2018PDT, vous devez ajouter manuellement une limite d'autorisation aux IAM rôles du projet. Comme meilleure pratique, nous vous recommandons d'utiliser une limite spécifique au projet qui comprend uniquement les ressources du projet pour éviter toute remontée des privilèges vers les ressources externes au projet. Suivez ces

étapes pour utiliser la limite d'autorisation AWS CodeStar gérée qui est mise à jour au fur et à mesure de l'évolution du projet.

1. Connectez-vous à la AWS CloudFormation console et recherchez le modèle pour la pile de chaînes d'outils dans votre projet. Ce modèle est nommé `awscodestar-project-id`.
2. Choisissez le modèle, Actions, puis Afficher/Modifier un modèle dans Designer.
3. Recherchez la section Resources et incluez l'extrait de code suivant en haut de la section.

```
PermissionsBoundaryPolicy:
  Description: Creating an IAM managed policy for defining the permissions boundary
for an AWS CodeStar project
  Type: AWS::IAM::ManagedPolicy
  Properties:
    ManagedPolicyName: !Sub 'CodeStar_${ProjectId }_PermissionsBoundary'
    Description: 'IAM policy to define the permissions boundary for IAM entities
created in an AWS CodeStar project'
    PolicyDocument:
      Version: '2012-10-17'
      Statement:
        - Sid: '1'
          Effect: Allow
          Action: ['*']
          Resource:
            - !Sub 'arn:${AWS::Partition}:cloudformation:${AWS::Region}:
${AWS::AccountId}:stack/awscodestar-${ProjectId}-*'

```

Vous aurez peut-être besoin d'IAM autorisations supplémentaires pour mettre à jour la pile depuis la AWS CloudFormation console.

4. (Facultatif) Si vous souhaitez créer des IAM rôles spécifiques à l'application, procédez comme suit. Depuis la IAM console, mettez à jour la politique intégrée associée au AWS CloudFormation rôle de votre projet afin d'inclure l'extrait de code suivant. Vous pourriez avoir besoin de IAM ressources supplémentaires pour mettre à jour la politique.

```
{
  "Action": [
    "iam:PassRole"
  ],

```

```

    "Resource": "arn:aws:iam::{AccountId}:role/CodeStar-{ProjectId}*",
    "Effect": "Allow"
  },
  {
    "Action": [
      "iam:CreateServiceLinkedRole",
      "iam:GetRole",
      "iam>DeleteRole",
      "iam>DeleteUser"
    ],
    "Resource": "*",
    "Effect": "Allow"
  },
  {
    "Action": [
      "iam:AttachRolePolicy",
      "iam:AttachUserPolicy",
      "iam:CreateRole",
      "iam:CreateUser",
      "iam>DeleteRolePolicy",
      "iam>DeleteUserPolicy",
      "iam:DetachUserPolicy",
      "iam:DetachRolePolicy",
      "iam:PutUserPermissionsBoundary",
      "iam:PutRolePermissionsBoundary"
    ],
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "iam:PermissionsBoundary": "arn:aws:iam::{AccountId}:policy/CodeStar_{ProjectId}_PermissionsBoundary"
      }
    },
    "Effect": "Allow"
  }
}

```

5. Appliquez une modification dans le pipeline de votre projet afin de mettre AWS CodeStar à jour la limite des autorisations avec les autorisations appropriées.

Pour de plus amples informations, veuillez consulter [Ajoutez un rôle IAM à un projet](#).

AWS CodeStar Exemples de politiques basées sur l'identité

Par défaut, IAM les utilisateurs et les rôles ne sont pas autorisés à créer ou à modifier AWS CodeStar des ressources. Ils ne peuvent pas non plus effectuer de tâches à l'aide du AWS Management Console AWS CLI, ou AWS API. Un administrateur doit créer des IAM politiques qui accordent aux utilisateurs et aux rôles l'autorisation d'effectuer des API opérations spécifiques sur les ressources spécifiques dont ils ont besoin. L'administrateur doit ensuite associer ces politiques aux IAM utilisateurs ou aux groupes qui ont besoin de ces autorisations.

Pour savoir comment créer une politique IAM basée sur l'identité à l'aide de ces exemples de documents de JSON stratégie, voir [Création de politiques dans l'JSONonglet du guide](#) de l'IAMutilisateur.

Rubriques

- [Bonnes pratiques en matière de politiques](#)
- [AWSCodeStarServiceRole Politique](#)
- [AWSCodeStarFullAccess Politique](#)
- [AWS CodeStar Politique relative au rôle du propriétaire](#)
- [Stratégie de rôle gérée par le participant AWS CodeStar](#)
- [AWS CodeStar Politique relative au rôle du spectateur](#)
- [AWS CodeStar Politique relative au rôle des travailleurs de la chaîne d'outils \(après le 6 décembre 2018PDT\)](#)
- [AWS CloudFormation Politique relative au rôle des travailleurs](#)
- [AWS CloudFormation Politique relative au rôle des travailleurs \(avant le 6 décembre 2018PDT\)](#)
- [AWS CodePipeline Politique relative au rôle des travailleurs \(avant le 6 décembre 2018PDT\)](#)
- [AWS CodeBuild Politique relative au rôle des travailleurs \(avant le 6 décembre 2018PDT\)](#)
- [Politique relative CloudWatch aux rôles des employés d'Amazon Events \(avant le 6 décembre 2018PDT\)](#)
- [AWS CodeStar Politique relative aux limites des autorisations](#)
- [Élaboration de la liste des ressources pour un projet](#)
- [Utilisation de la AWS CodeStar console](#)
- [Autoriser les utilisateurs à afficher leurs propres autorisations](#)
- [Mise à jour d'un projet AWS CodeStar](#)
- [Ajout d'un membre d'équipe à un projet](#)

- [Répertorier les profils d'utilisateurs associés à un AWS compte](#)
- [Affichage des projets AWS CodeStar en fonction des balises](#)
- [AWS CodeStar mises à jour des politiques AWS gérées](#)

Bonnes pratiques en matière de politiques

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

- Commencez AWS par les politiques gérées et passez aux autorisations du moindre privilège : pour commencer à accorder des autorisations à vos utilisateurs et à vos charges de travail, utilisez les politiques AWS gérées qui accordent des autorisations pour de nombreux cas d'utilisation courants. Ils sont disponibles dans votre Compte AWS. Nous vous recommandons de réduire davantage les autorisations en définissant des politiques gérées par les AWS clients spécifiques à vos cas d'utilisation. Pour plus d'informations, consultez [les politiques AWS gérées ou les politiques AWS gérées pour les fonctions professionnelles](#) dans le Guide de IAM l'utilisateur.
- Appliquer les autorisations du moindre privilège : lorsque vous définissez des autorisations à IAM l'aide de politiques, accordez uniquement les autorisations nécessaires à l'exécution d'une tâche. Pour ce faire, vous définissez les actions qui peuvent être entreprises sur des ressources spécifiques dans des conditions spécifiques, également appelées autorisations de moindre privilège. Pour plus d'informations sur l'utilisation IAM pour appliquer des autorisations, consultez la section [Politiques et autorisations](#) du Guide de IAM l'utilisateur. IAM
- Utilisez des conditions dans IAM les politiques pour restreindre davantage l'accès : vous pouvez ajouter une condition à vos politiques pour limiter l'accès aux actions et aux ressources. Par exemple, vous pouvez rédiger une condition de politique pour spécifier que toutes les demandes doivent être envoyées en utilisant SSL. Vous pouvez également utiliser des conditions pour accorder l'accès aux actions de service si elles sont utilisées par le biais d'un service spécifique Service AWS, tel que AWS CloudFormation. Pour plus d'informations, voir [Éléments IAM JSON de politique : Condition](#) dans le guide de IAM l'utilisateur.
- Utilisez IAM Access Analyzer pour valider vos IAM politiques afin de garantir des autorisations sécurisées et fonctionnelles. IAM Access Analyzer valide les politiques nouvelles et existantes afin qu'elles respectent le langage des politiques (JSON) et IAM les IAM meilleures pratiques. IAM Access Analyzer fournit plus de 100 vérifications des politiques et des recommandations exploitables pour vous aider à créer des politiques sécurisées et fonctionnelles. Pour plus

d'informations, consultez la section [Validation des politiques d'IAccess Analyzer](#) dans le guide de IAM l'utilisateur.

- Exiger l'authentification multifactorielle (MFA) : si vous avez un scénario qui nécessite des IAM utilisateurs ou un utilisateur root Compte AWS, activez-le MFA pour une sécurité supplémentaire. Pour exiger le MFA moment où les API opérations sont appelées, ajoutez MFA des conditions à vos politiques. Pour plus d'informations, consultez [la section Configuration de l'API accès MFA protégé](#) dans le Guide de l'IAMutilisateur.

Pour plus d'informations sur les meilleures pratiques en matière de [sécuritéIAM](#), consultez la section [Bonnes pratiques en matière](#) de sécurité IAM dans le Guide de IAM l'utilisateur.

AWSCodeStarServiceRole Politique

La `aws-codestar-service-role` politique est attachée au rôle de service qui permet d' AWS CodeStar effectuer des actions avec d'autres services. La première fois que vous vous connectez à AWS CodeStar, vous créez le rôle de service. Vous n'avez besoin de le créer qu'une seule fois. La stratégie est automatiquement attachée au rôle de service après sa création.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ProjectEventRules",
      "Effect": "Allow",
      "Action": [
        "events:PutTargets",
        "events:RemoveTargets",
        "events:PutRule",
        "events>DeleteRule",
        "events:DescribeRule"
      ],
      "Resource": [
        "arn:aws:events:*:*:rule/awscodestar-*"
      ]
    },
    {
      "Sid": "ProjectStack",
      "Effect": "Allow",
      "Action": [
        "cloudformation:*Stack*",
        "cloudformation:CreateChangeSet",

```

```

        "cloudformation:ExecuteChangeSet",
        "cloudformation>DeleteChangeSet",
        "cloudformation:GetTemplate"
    ],
    "Resource": [
        "arn:aws:cloudformation:*:*:stack/awscodestar-*",
        "arn:aws:cloudformation:*:*:stack/awseb-*",
        "arn:aws:cloudformation:*:*:stack/aws-cloud9-*",
        "arn:aws:cloudformation:*:aws:transform/CodeStar*"
    ]
},
{
    "Sid": "ProjectStackTemplate",
    "Effect": "Allow",
    "Action": [
        "cloudformation:GetTemplateSummary",
        "cloudformation:DescribeChangeSet"
    ],
    "Resource": "*"
},
{
    "Sid": "ProjectQuickstarts",
    "Effect": "Allow",
    "Action": [
        "s3:GetObject"
    ],
    "Resource": [
        "arn:aws:s3:::awscodestar-*/*"
    ]
},
{
    "Sid": "ProjectS3Buckets",
    "Effect": "Allow",
    "Action": [
        "s3:*"
    ],
    "Resource": [
        "arn:aws:s3:::aws-codestar-*",
        "arn:aws:s3:::elasticbeanstalk-*"
    ]
},
{
    "Sid": "ProjectServices",
    "Effect": "Allow",

```

```

    "Action": [
      "codestar:*",
      "codecommit:*",
      "codepipeline:*",
      "codedeploy:*",
      "codebuild:*",
      "autoscaling:*",
      "cloudwatch:Put*",
      "ec2:*",
      "elasticbeanstalk:*",
      "elasticloadbalancing:*",
      "iam:ListRoles",
      "logs:*",
      "sns:*",
      "cloud9:CreateEnvironmentEC2",
      "cloud9>DeleteEnvironment",
      "cloud9:DescribeEnvironment*",
      "cloud9:ListEnvironments"
    ],
    "Resource": "*"
  },
  {
    "Sid": "ProjectWorkerRoles",
    "Effect": "Allow",
    "Action": [
      "iam:AttachRolePolicy",
      "iam:CreateRole",
      "iam>DeleteRole",
      "iam>DeleteRolePolicy",
      "iam:DetachRolePolicy",
      "iam:GetRole",
      "iam:PassRole",
      "iam:GetRolePolicy",
      "iam:PutRolePolicy",
      "iam:SetDefaultPolicyVersion",
      "iam:CreatePolicy",
      "iam>DeletePolicy",
      "iam:AddRoleToInstanceProfile",
      "iam:CreateInstanceProfile",
      "iam>DeleteInstanceProfile",
      "iam:RemoveRoleFromInstanceProfile"
    ],
    "Resource": [
      "arn:aws:iam::*:role/CodeStarWorker*"
    ]
  }

```

```

        "arn:aws:iam::*:policy/CodeStarWorker*",
        "arn:aws:iam::*:instance-profile/awscodestar-*"
    ]
},
{
    "Sid": "ProjectTeamMembers",
    "Effect": "Allow",
    "Action": [
        "iam:AttachUserPolicy",
        "iam:DetachUserPolicy"
    ],
    "Resource": "*",
    "Condition": {
        "ArnEquals": {
            "iam:PolicyArn": [
                "arn:aws:iam::*:policy/CodeStar_*"
            ]
        }
    }
},
{
    "Sid": "ProjectRoles",
    "Effect": "Allow",
    "Action": [
        "iam:CreatePolicy",
        "iam>DeletePolicy",
        "iam:CreatePolicyVersion",
        "iam>DeletePolicyVersion",
        "iam>ListEntitiesForPolicy",
        "iam>ListPolicyVersions",
        "iam:GetPolicy",
        "iam:GetPolicyVersion"
    ],
    "Resource": [
        "arn:aws:iam::*:policy/CodeStar_*"
    ]
},
{
    "Sid": "InspectServiceRole",
    "Effect": "Allow",
    "Action": [
        "iam>ListAttachedRolePolicies"
    ],
    "Resource": [

```



```

        "arn:aws:iam::*:role/aws-codestar-service-role",
        "arn:aws:iam::*:role/service-role/aws-codestar-service-role"
    ]
},
{
    "Sid": "IAMLinkRole",
    "Effect": "Allow",
    "Action": [
        "iam:CreateServiceLinkedRole"
    ],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "iam:AWSServiceName": "cloud9.amazonaws.com"
        }
    }
},
{
    "Sid": "DescribeConfigRuleForARN",
    "Effect": "Allow",
    "Action": [
        "config:DescribeConfigRules"
    ],
    "Resource": [
        "*"
    ]
},
{
    "Sid": "ProjectCodeStarConnections",
    "Effect": "Allow",
    "Action": [
        "codestar-connections:UseConnection",
        "codestar-connections:GetConnection"
    ],
    "Resource": "*"
},
{
    "Sid": "ProjectCodeStarConnectionsPassConnections",
    "Effect": "Allow",
    "Action": "codestar-connections:PassConnection",
    "Resource": "*",
    "Condition": {
        "StringEqualsIfExists": {

```

```
        "codestar-connections:PassedToService":
    "codepipeline.amazonaws.com"
        }
    }
}
]
```

AWSCodeStarFullAccess Politique

Dans les [Configuration AWS CodeStar](#) instructions, vous avez joint une politique nommée `AWSCodeStarFullAccess` à votre IAM utilisateur. Cette déclaration de politique permet à l'utilisateur d'effectuer toutes les actions disponibles AWS CodeStar avec toutes les AWS CodeStar ressources disponibles associées au AWS compte. Cela comprend également la création et la suppression de projets. L'exemple suivant est un extrait d'une stratégie `AWSCodeStarFullAccess` représentative. La politique réelle varie en fonction du modèle que vous sélectionnez lorsque vous démarrez un nouveau AWS CodeStar projet.

AWS CloudFormation nécessite une `cloudformation::ListStacks` autorisation lors d'un appel `cloudformation::DescribeStacks` sans pile cible.

Détails de l'autorisation

Cette politique inclut les autorisations permettant d'effectuer les opérations suivantes :

- `ec2`—Récupérez des informations sur EC2 les instances pour créer un AWS CodeStar projet.
- `cloud9`—Récupérez des informations sur les AWS Command Line Interface environnements.
- `cloudformation`—Récupérez des informations sur les piles AWS CodeStar de projets.
- `codestar`—Réaliser des actions dans le cadre d'un AWS CodeStar projet.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "CodeStarEC2",
      "Effect": "Allow",
      "Action": [
        "codestar:*",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeVpcs",
```

```

    "ec2:DescribeSubnets",
    "cloud9:DescribeEnvironment*"
  ],
  "Resource": "*"
},
{
  "Sid": "CodeStarCF",
  "Effect": "Allow",
  "Action": [
    "cloudformation:DescribeStack*",
    "cloudformation:ListStacks*",
    "cloudformation:GetTemplateSummary"
  ],
  "Resource": [
    "arn:aws:cloudformation:*:*:stack/awscodestar-*"
  ]
}
]
}

```

Vous ne voudrez peut-être pas accorder un tel accès à tous les utilisateurs. Vous pouvez plutôt ajouter des autorisations au niveau du projet à l'aide des rôles de projet gérés par AWS CodeStar. Les rôles accordent des niveaux d'accès spécifiques aux AWS CodeStar projets et sont nommés comme suit :

- Propriétaire
- Participant
- Lecteur

AWS CodeStar Politique relative au rôle du propriétaire

La politique AWS CodeStar du rôle du propriétaire permet à un utilisateur d'effectuer toutes les actions d'un AWS CodeStar projet sans aucune restriction. AWS CodeStar applique la `CodeStar_project-id_Owner` politique aux membres de l'équipe de projet ayant le niveau d'accès propriétaire.

```

...
{
  "Effect": "Allow",
  "Action": [

```

```

...
"codestar:*",
...
],
"Resource": [
  "arn:aws:codestar:us-east-2:111111111111:project/project-id",
  "arn:aws:iam::account-id:policy/CodeStar_project-id_Owner"
]
},
{
  "Effect": "Allow",
  "Action": [
    "codestar:DescribeUserProfile",
    "codestar:ListProjects",
    "codestar:ListUserProfiles",
    "codestar:VerifyServiceRole",
    ...
  ],
  "Resource": [
    "*"
  ]
},
{
  "Effect": "Allow",
  "Action": [
    "codestar:*UserProfile",
    ...
  ],
  "Resource": [
    "arn:aws:iam::account-id:user/user-name"
  ]
}
...

```

Stratégie de rôle gérée par le participant AWS CodeStar

La politique relative aux rôles de AWS CodeStar contributeur permet à un utilisateur de contribuer au projet et de modifier le tableau de bord du projet. AWS CodeStar applique la `CodeStar_project-id_Contributor` politique aux membres de l'équipe de projet ayant le niveau d'accès du contributeur. Les utilisateurs à accès de participant peuvent contribuer au projet et modifier son tableau de bord, mais ne peuvent pas ajouter ou supprimer des membres de l'équipe.

...

```
{
  "Effect": "Allow",
  "Action": [
    ...
    "codestar:Describe*",
    "codestar:Get*",
    "codestar:List*",
    "codestar:PutExtendedAccess",
    ...
  ],
  "Resource": [
    "arn:aws:codestar:us-east-2:111111111111:project/project-id",
    "arn:aws:iam::account-id:policy/CodeStar_project-id_Contributor"
  ]
},
{
  "Effect": "Allow",
  "Action": [
    "codestar:DescribeUserProfile",
    "codestar:ListProjects",
    "codestar:ListUserProfiles",
    "codestar:VerifyServiceRole",
    ...
  ],
  "Resource": [
    "*"
  ]
},
{
  "Effect": "Allow",
  "Action": [
    "codestar:*UserProfile",
    ...
  ],
  "Resource": [
    "arn:aws:iam::account-id:user/user-name"
  ]
}
...
```

AWS CodeStar Politique relative au rôle du spectateur

La politique relative au rôle du AWS CodeStar spectateur permet à un utilisateur de visualiser un projet dans AWS CodeStar. AWS CodeStar applique la CodeStar_*project-id*_Viewer politique aux membres de l'équipe de projet ayant le niveau d'accès des spectateurs. Les utilisateurs ayant accès à un lecteur peuvent consulter un projet AWS CodeStar, mais ils ne peuvent pas modifier ses ressources ni ajouter ou supprimer des membres de l'équipe.

```
...
{
  "Effect": "Allow",
  "Action": [
    ...
    "codestar:Describe*",
    "codestar:Get*",
    "codestar:List*",
    ...
  ],
  "Resource": [
    "arn:aws:codestar:us-east-2:111111111111:project/project-id",
    "arn:aws:iam:account-id:policy/CodeStar_project-id_Viewer"
  ]
},
{
  "Effect": "Allow",
  "Action": [
    "codestar:DescribeUserProfile",
    "codestar:ListProjects",
    "codestar:ListUserProfiles",
    "codestar:VerifyServiceRole",
    ...
  ],
  "Resource": [
    "*"
  ]
},
{
  "Effect": "Allow",
  "Action": [
    "codestar:*UserProfile",
    ...
  ],
  "Resource": [
```

```
"arn:aws:iam::account-id:user/user-name"
]
}
...
```

AWS CodeStar Politique relative au rôle des travailleurs de la chaîne d'outils (après le 6 décembre 2018PDT)

Pour les AWS CodeStar projets créés après le 6 décembre 2018PDT, AWS CodeStar crée une politique intégrée pour un rôle de travailleur qui crée des ressources pour votre projet dans d'autres AWS services. Le contenu de cette stratégie dépend du type de projet que vous créez. La stratégie suivante est un exemple. Pour de plus amples informations, veuillez consulter [IAM Politiques relatives aux rôles des travailleurs](#).

```
{
  "Statement": [
    {
      "Action": [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:GetBucketVersioning",
        "s3:PutObject*",
        "codecommit:CancelUploadArchive",
        "codecommit:GetBranch",
        "codecommit:GetCommit",
        "codecommit:GetUploadArchiveStatus",
        "codecommit:GitPull",
        "codecommit:UploadArchive",
        "codebuild:StartBuild",
        "codebuild:BatchGetBuilds",
        "codebuild:StopBuild",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeChangeSet",
        "cloudformation:CreateChangeSet",
        "cloudformation>DeleteChangeSet",
        "cloudformation:ExecuteChangeSet",
        "codepipeline:StartPipelineExecution",
        "lambda:ListFunctions",
        "lambda:InvokeFunction",
```

```

    "sns:Publish"
  ],
  "Resource": [
    "*"
  ],
  "Effect": "Allow"
},
{
  "Action": [
    "iam:PassRole"
  ],
  "Resource": [
    "*"
  ],
  "Effect": "Allow"
},
{
  "Action": [
    "kms:GenerateDataKey*",
    "kms:Encrypt",
    "kms:Decrypt"
  ],
  "Resource": [
    "*"
  ],
  "Effect": "Allow"
}
]
}

```

AWS CloudFormation Politique relative au rôle des travailleurs

Pour les AWS CodeStar projets créés après le 6 décembre 2018PDT, AWS CodeStar crée une politique intégrée pour un rôle de travailleur qui crée AWS CloudFormation des ressources pour votre AWS CodeStar projet. Le contenu de la stratégie dépend du type de ressources requis pour votre projet. La stratégie suivante est un exemple. Pour de plus amples informations, veuillez consulter [IAM Politiques relatives aux rôles des travailleurs](#).

```

{
{
  "Statement": [
    {

```



```

    "Action": [
      "s3:PutObject",
      "s3:GetObject",
      "s3:GetObjectVersion"
    ],
    "Resource": [
      "arn:aws:s3::aws-codestar-region-id-account-id-project-id",
      "arn:aws:s3::aws-codestar-region-id-account-id-project-id/*"
    ],
    "Effect": "Allow"
  },
  {
    "Action": [
      "apigateway:DELETE",
      "apigateway:GET",
      "apigateway:PATCH",
      "apigateway:POST",
      "apigateway:PUT",
      "codedeploy:CreateApplication",
      "codedeploy:CreateDeployment",
      "codedeploy:CreateDeploymentConfig",
      "codedeploy:CreateDeploymentGroup",
      "codedeploy>DeleteApplication",
      "codedeploy>DeleteDeployment",
      "codedeploy>DeleteDeploymentConfig",
      "codedeploy>DeleteDeploymentGroup",
      "codedeploy:GetDeployment",
      "codedeploy:GetDeploymentConfig",
      "codedeploy:GetDeploymentGroup",
      "codedeploy:RegisterApplicationRevision",
      "codestar:SyncResources",
      "config>DeleteConfigRule",
      "config:DescribeConfigRules",
      "config:ListTagsForResource",
      "config:PutConfigRule",
      "config:TagResource",
      "config:UntagResource",
      "dynamodb>CreateTable",
      "dynamodb>DeleteTable",
      "dynamodb:DescribeContinuousBackups",
      "dynamodb:DescribeTable",
      "dynamodb:DescribeTimeToLive",
      "dynamodb:ListTagsOfResource",
      "dynamodb:TagResource",

```

```
"dynamodb:UntagResource",
"dynamodb:UpdateContinuousBackups",
"dynamodb:UpdateTable",
"dynamodb:UpdateTimeToLive",
"ec2:AssociateIamInstanceProfile",
"ec2:AttachVolume",
"ec2:CreateSecurityGroup",
"ec2:createTags",
"ec2:DescribeIamInstanceProfileAssociations",
"ec2:DescribeInstances",
"ec2:DescribeSecurityGroups",
"ec2:DescribeSubnets",
"ec2:DetachVolume",
"ec2:DisassociateIamInstanceProfile",
"ec2:ModifyInstanceAttribute",
"ec2:ModifyInstanceCreditSpecification",
"ec2:ModifyInstancePlacement",
"ec2:MonitorInstances",
"ec2:ReplaceIamInstanceProfileAssociation",
"ec2:RunInstances",
"ec2:StartInstances",
"ec2:StopInstances",
"ec2:TerminateInstances",
"events:DeleteRule",
"events:DescribeRule",
"events:ListTagsForResource",
"events:PutRule",
"events:PutTargets",
"events:RemoveTargets",
"events:TagResource",
"events:UntagResource",
"kinesis:AddTagsToStream",
"kinesis:CreateStream",
"kinesis:DecreaseStreamRetentionPeriod",
"kinesis>DeleteStream",
"kinesis:DescribeStream",
"kinesis:IncreaseStreamRetentionPeriod",
"kinesis:RemoveTagsFromStream",
"kinesis:StartStreamEncryption",
"kinesis:StopStreamEncryption",
"kinesis:UpdateShardCount",
"lambda:CreateAlias",
"lambda:CreateFunction",
"lambda>DeleteAlias",
```

```
"lambda:DeleteFunction",
"lambda:DeleteFunctionConcurrency",
"lambda:GetFunction",
"lambda:GetFunctionConfiguration",
"lambda:ListTags",
"lambda:ListVersionsByFunction",
"lambda:PublishVersion",
"lambda:PutFunctionConcurrency",
"lambda:TagResource",
"lambda:UntagResource",
"lambda:UpdateAlias",
"lambda:UpdateFunctionCode",
"lambda:UpdateFunctionConfiguration",
"s3:CreateBucket",
"s3:DeleteBucket",
"s3:DeleteBucketWebsite",
"s3:PutAccelerateConfiguration",
"s3:PutAnalyticsConfiguration",
"s3:PutBucketAcl",
"s3:PutBucketCORS",
"s3:PutBucketLogging",
"s3:PutBucketNotification",
"s3:PutBucketPublicAccessBlock",
"s3:PutBucketVersioning",
"s3:PutBucketWebsite",
"s3:PutEncryptionConfiguration",
"s3:PutInventoryConfiguration",
"s3:PutLifecycleConfiguration",
"s3:PutMetricsConfiguration",
"s3:PutReplicationConfiguration",
"sns:CreateTopic",
"sns:DeleteTopic",
"sns:GetTopicAttributes",
"sns:ListSubscriptionsByTopic",
"sns:ListTopics",
"sns:SetSubscriptionAttributes",
"sns:Subscribe",
"sns:Unsubscribe",
"sqs:CreateQueue",
"sqs:DeleteQueue",
"sqs:GetQueueAttributes",
"sqs:GetQueueUrl",
"sqs:ListQueueTags",
"sqs:TagQueue",
```

```

        "sqs:UntagQueue"
    ],
    "Resource": "*",
    "Effect": "Allow"
},
{
    "Action": [
        "lambda:AddPermission",
        "lambda:RemovePermission"
    ],
    "Resource": [
        "arn:aws:lambda:region-id:account-id:function:awscodestar-*"
    ],
    "Effect": "Allow"
},
{
    "Action": [
        "iam:PassRole"
    ],
    "Resource": [
        "arn:aws:iam::account-id:role/CodeStar-project-id*"
    ],
    "Effect": "Allow"
},
{
    "Condition": {
        "StringEquals": {
            "iam:PassedToService": "codedeploy.amazonaws.com"
        }
    },
    "Action": [
        "iam:PassRole"
    ],
    "Resource": [
        "arn:aws:iam::account-id:role/CodeStarWorker-project-id-CodeDeploy"
    ],
    "Effect": "Allow"
},
{
    "Action": [
        "cloudformation:CreateChangeSet"
    ],
    "Resource": [
        "arn:aws:cloudformation:region-id:aws:transform/Serverless-2016-10-31",

```

```

        "arn:aws:cloudformation:region-id:aws:transform/CodeStar"
    ],
    "Effect": "Allow"
},
{
    "Action": [
        "iam:CreateServiceLinkedRole",
        "iam:GetRole",
        "iam>DeleteRole",
        "iam>DeleteUser"
    ],
    "Resource": "*",
    "Effect": "Allow"
},
{
    "Condition": {
        "StringEquals": {
            "iam:PermissionsBoundary": "arn:aws:iam::account-id:policy/
CodeStar_project-id_PermissionsBoundary"
        }
    },
    "Action": [
        "iam:AttachRolePolicy",
        "iam:AttachUserPolicy",
        "iam:CreateRole",
        "iam:CreateUser",
        "iam>DeleteRolePolicy",
        "iam>DeleteUserPolicy",
        "iam:DetachUserPolicy",
        "iam:DetachRolePolicy",
        "iam:PutUserPermissionsBoundary",
        "iam:PutRolePermissionsBoundary"
    ],
    "Resource": "*",
    "Effect": "Allow"
},
{
    "Action": [
        "kms:CreateKey",
        "kms:CreateAlias",
        "kms>DeleteAlias",
        "kms:DisableKey",
        "kms:EnableKey",
        "kms:UpdateAlias",

```

```

        "kms:TagResource",
        "kms:UntagResource"
    ],
    "Resource": "*",
    "Effect": "Allow"
},
{
    "Condition": {
        "StringEquals": {
            "ssm:ResourceTag/awscodestar:projectArn":
"arn:aws:codestar:project-id:account-id:project/project-id"
        }
    },
    "Action": [
        "ssm:GetParameter*"
    ],
    "Resource": "*",
    "Effect": "Allow"
}
]
}

```

AWS CloudFormation Politique relative au rôle des travailleurs (avant le 6 décembre 2018PDT)

Si votre AWS CodeStar projet a été créé avant le 6 décembre 2018PDT, AWS CodeStar crée une politique intégrée pour un rôle de AWS CloudFormation travailleur. La déclaration de stratégie suivante est un exemple.

```

{
  "Statement": [
    {
      "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource": [
        "arn:aws:s3::aws-codestar-us-east-1-account-id-project-id-pipe",
        "arn:aws:s3::aws-codestar-us-east-1-account-id-project-id-pipe/*"
      ],
      "Effect": "Allow"
    }
  ]
}

```

```
    },
    {
      "Action": [
        "codestar:SyncResources",
        "lambda:CreateFunction",
        "lambda>DeleteFunction",
        "lambda:AddPermission",
        "lambda:UpdateFunction",
        "lambda:UpdateFunctionCode",
        "lambda:GetFunction",
        "lambda:GetFunctionConfiguration",
        "lambda:UpdateFunctionConfiguration",
        "lambda:RemovePermission",
        "lambda:listTags",
        "lambda:TagResource",
        "lambda:UntagResource",
        "apigateway:*",
        "dynamodb:CreateTable",
        "dynamodb>DeleteTable",
        "dynamodb:DescribeTable",
        "kinesis:CreateStream",
        "kinesis>DeleteStream",
        "kinesis:DescribeStream",
        "sns:CreateTopic",
        "sns>DeleteTopic",
        "sns:ListTopics",
        "sns:GetTopicAttributes",
        "sns:SetTopicAttributes",
        "s3:CreateBucket",
        "s3>DeleteBucket",
        "config:DescribeConfigRules",
        "config:PutConfigRule",
        "config>DeleteConfigRule",
        "ec2:*",
        "autoscaling:*",
        "elasticloadbalancing:*",
        "elasticbeanstalk:*"
      ],
      "Resource": "*",
      "Effect": "Allow"
    },
    {
      "Action": [
        "iam:PassRole"
```

```

    ],
    "Resource": [
      "arn:aws:iam::account-id:role/CodeStarWorker-project-id-Lambda"
    ],
    "Effect": "Allow"
  },
  {
    "Action": [
      "cloudformation:CreateChangeSet"
    ],
    "Resource": [
      "arn:aws:cloudformation:us-east-1:aws:transform/Serverless-2016-10-31",
      "arn:aws:cloudformation:us-east-1:aws:transform/CodeStar"
    ],
    "Effect": "Allow"
  }
]
}

```

AWS CodePipeline Politique relative au rôle des travailleurs (avant le 6 décembre 2018PDT)

Si votre AWS CodeStar projet a été créé avant le 6 décembre 2018PDT, AWS CodeStar crée une politique intégrée pour un rôle de CodePipeline travailleur. La déclaration de stratégie suivante est un exemple.

```

{
  "Statement": [
    {
      "Action": [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:GetBucketVersioning",
        "s3:PutObject"
      ],
      "Resource": [
        "arn:aws:s3::aws-codestar-us-east-1-account-id-project-id-pipe",
        "arn:aws:s3::aws-codestar-us-east-1-account-id-project-id-pipe/*"
      ],
      "Effect": "Allow"
    },
    {
      "Action": [

```



```

        "codecommit:CancelUploadArchive",
        "codecommit:GetBranch",
        "codecommit:GetCommit",
        "codecommit:GetUploadArchiveStatus",
        "codecommit:UploadArchive"
    ],
    "Resource": [
        "arn:aws:codecommit:us-east-1:account-id:project-id"
    ],
    "Effect": "Allow"
},
{
    "Action": [
        "codebuild:StartBuild",
        "codebuild:BatchGetBuilds",
        "codebuild:StopBuild"
    ],
    "Resource": [
        "arn:aws:codebuild:us-east-1:account-id:project/project-id"
    ],
    "Effect": "Allow"
},
{
    "Action": [
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeChangeSet",
        "cloudformation:CreateChangeSet",
        "cloudformation>DeleteChangeSet",
        "cloudformation:ExecuteChangeSet"
    ],
    "Resource": [
        "arn:aws:cloudformation:us-east-1:account-id:stack/awscodestar-project-id-lambda/*"
    ],
    "Effect": "Allow"
},
{
    "Action": [
        "iam:PassRole"
    ],
    "Resource": [
        "arn:aws:iam::account-id:role/CodeStarWorker-project-id-CloudFormation"
    ],
    "Effect": "Allow"
}

```

```

    }
  ]
}

```

AWS CodeBuild Politique relative au rôle des travailleurs (avant le 6 décembre 2018PDT)

Si votre AWS CodeStar projet a été créé avant le 6 décembre 2018PDT, AWS CodeStar crée une politique intégrée pour un rôle de CodeBuild travailleur. La déclaration de stratégie suivante est un exemple.

```

{
  "Statement": [
    {
      "Action": [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource": "*",
      "Effect": "Allow"
    },
    {
      "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource": [
        "arn:aws:s3::aws-codestar-us-east-1-account-id-project-id-pipe",
        "arn:aws:s3::aws-codestar-us-east-1-account-id-project-id-pipe/*",
        "arn:aws:s3::aws-codestar-us-east-1-account-id-project-id-app",
        "arn:aws:s3::aws-codestar-us-east-1-account-id-project-id-app/*"
      ],
      "Effect": "Allow"
    },
    {
      "Action": [
        "codecommit:GitPull"
      ],
      "Resource": [
        "arn:aws:codecommit:us-east-1:account-id:project-id"
      ],
    }
  ]
}

```

```

    "Effect": "Allow"
  },
  {
    "Action": [
      "kms:GenerateDataKey*",
      "kms:Encrypt",
      "kms:Decrypt"
    ],
    "Resource": [
      "arn:aws:kms:us-east-1:account-id:alias/aws/s3"
    ],
    "Effect": "Allow"
  }
]
}

```

Politique relative CloudWatch aux rôles des employés d'Amazon Events (avant le 6 décembre 2018PDT)

Si votre AWS CodeStar projet a été créé avant le 6 décembre 2018PDT, créez AWS CodeStar une politique intégrée pour un rôle de travailleur CloudWatch événementiel. La déclaration de stratégie suivante est un exemple.

```

{
  "Statement": [
    {
      "Action": [
        "codepipeline:StartPipelineExecution"
      ],
      "Resource": [
        "arn:aws:codepipeline:us-east-1:account-id:project-id-Pipeline"
      ],
      "Effect": "Allow"
    }
  ]
}

```

AWS CodeStar Politique relative aux limites des autorisations

Si vous créez un AWS CodeStar projet après le 6 décembre 2018PDT, AWS CodeStar crée une politique de limites d'autorisations pour votre projet. Cette stratégie empêche l'escalade des privilèges

à des ressources en dehors du projet. Il s'agit d'une stratégie dynamique qui est mise à jour au fur et à mesure que le projet évolue. Le contenu de cette stratégie dépend du type de projet que vous créez. La stratégie suivante est un exemple. Pour de plus amples informations, veuillez consulter [Limite d'autorisations IAM](#).

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "1",
      "Effect": "Allow",
      "Action": [
        "s3:GetObject"
      ],
      "Resource": [
        "arn:aws:s3::*/AWSLogs/*/Config/*"
      ]
    },
    {
      "Sid": "2",
      "Effect": "Allow",
      "Action": [
        "*"
      ],
      "Resource": [
        "arn:aws:codestar:us-east-1:account-id:project/project-id",
        "arn:aws:cloudformation:us-east-1:account-id:stack/awscodestar-project-id-lambda/eefbbf20-c1d9-11e8-8a3a-500c28b4e461",
        "arn:aws:cloudformation:us-east-1:account-id:stack/awscodestar-project-id/4b80b3f0-c1d9-11e8-8517-500c28b236fd",
        "arn:aws:codebuild:us-east-1:account-id:project/project-id",
        "arn:aws:codecommit:us-east-1:account-id:project-id",
        "arn:aws:codepipeline:us-east-1:account-id:project-id-Pipeline",
        "arn:aws:execute-api:us-east-1:account-id:7rlst5mrgi",
        "arn:aws:iam::account-id:role/CodeStarWorker-project-id-CloudFormation",
        "arn:aws:iam::account-id:role/CodeStarWorker-project-id-CloudWatchEventRule",
        "arn:aws:iam::account-id:role/CodeStarWorker-project-id-CodeBuild",
        "arn:aws:iam::account-id:role/CodeStarWorker-project-id-CodePipeline",
        "arn:aws:iam::account-id:role/CodeStarWorker-project-id-Lambda",
        "arn:aws:lambda:us-east-1:account-id:function:awscodestar-project-id-lambda-GetHelloWorld-KFKTXYNH9573",
        "arn:aws:s3::aws-codestar-us-east-1-account-id-project-id-app",
        "arn:aws:s3::aws-codestar-us-east-1-account-id-project-id-pipe"
      ]
    }
  ]
}
```

```
    ]
  },
  {
    "Sid": "3",
    "Effect": "Allow",
    "Action": [
      "apigateway:GET",
      "config:Describe*",
      "config:Get*",
      "config:List*",
      "config:Put*",
      "logs:CreateLogGroup",
      "logs:CreateLogStream",
      "logs:DescribeLogGroups",
      "logs:PutLogEvents"
    ],
    "Resource": [
      "*"
    ]
  }
]
```

Élaboration de la liste des ressources pour un projet

Dans cet exemple, vous souhaitez autoriser un IAM utilisateur spécifique de votre AWS compte à accéder à la liste des ressources d'un AWS CodeStar projet.

```
{
  "Version": "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "codestar:ListResources",
      ],
      "Resource" : "arn:aws:codestar:us-east-2:project/my-first-projec"
    }
  ]
}
```

Utilisation de la AWS CodeStar console

Aucune autorisation spécifique n'est requise pour accéder à la AWS CodeStar console, mais vous ne pouvez rien faire d'utile si vous n'avez pas la `AWSCodeStarFullAccess` politique ou l'un des rôles AWS CodeStar au niveau du projet : propriétaire, contributeur ou spectateur. Pour plus d'informations sur `AWSCodeStarFullAccess`, consultez [AWSCodeStarFullAccess Politique](#). Pour de plus amples informations sur les stratégies au niveau du projet, veuillez consulter [IAM Politiques pour les membres de l'équipe](#).

Il n'est pas nécessaire d'accorder des autorisations de console minimales aux utilisateurs qui passent des appels uniquement vers le AWS CLI ou le AWS API. Au lieu de cela, autorisez uniquement l'accès aux actions correspondant à l'API opération que vous essayez d'effectuer.

Autoriser les utilisateurs à afficher leurs propres autorisations

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

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ViewOwnUserInfo",
      "Effect": "Allow",
      "Action": [
        "iam:GetUserPolicy",
        "iam:ListGroupsWithUser",
        "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": "*"
}
]
}

```

Mise à jour d'un projet AWS CodeStar

Dans cet exemple, vous souhaitez autoriser un IAM utilisateur spécifique de votre AWS compte à modifier les attributs d'un AWS CodeStar projet, tels que sa description.

```

{
  "Version": "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "codestar:UpdateProject"
      ],
      "Resource" : "arn:aws:codestar:us-east-2:project/my-first-projec"
    }
  ]
}

```

Ajout d'un membre d'équipe à un projet

Dans cet exemple, vous souhaitez autoriser un IAM utilisateur spécifique à ajouter des membres de l'équipe à un AWS CodeStar projet avec l'ID du projet *my-first-projec*, mais pour refuser explicitement à cet utilisateur la possibilité de supprimer des membres de l'équipe :

```

{
  "Version": "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "codestar:AssociateTeamMember",

```

```

    ],
    "Resource" : "arn:aws:codestar:us-east-2:project/my-first-projec"
  },
  {
    "Effect" : "Deny",
    "Action" : [
      "codestar:DisassociateTeamMember",
    ],
    "Resource" : "arn:aws:codestar:us-east-2:project/my-first-projec"
  }
]
}

```

Répertorier les profils d'utilisateurs associés à un AWS compte

Dans cet exemple, vous autorisez un IAM utilisateur auquel cette politique est attachée à répertorier tous les profils AWS CodeStar utilisateur associés à un AWS compte :

```

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

```

Affichage des projets AWS CodeStar en fonction des balises

Vous pouvez utiliser des conditions dans votre politique basée sur l'identité pour contrôler l'accès aux AWS CodeStar projets en fonction de balises. Cet exemple montre comment créer une stratégie qui autorise l'affichage d'un projet. Toutefois, l'autorisation est accordée uniquement si la balise de projet Owner a la valeur du nom d'utilisateur de cet utilisateur. Cette politique accorde également les autorisations nécessaires pour réaliser cette action sur la console.

```

{

```



```

"Version": "2012-10-17",
"Statement": [
  {
    "Sid": "ListProjectsInConsole",
    "Effect": "Allow",
    "Action": "codestar:ListProjects",
    "Resource": "*"
  },
  {
    "Sid": "ViewProjectIfOwner",
    "Effect": "Allow",
    "Action": "codestar:GetProject",
    "Resource": "arn:aws:codestar:*:*:project/*",
    "Condition": {
      "StringEquals": {"codestar:ResourceTag/Owner": "${aws:username}"}
    }
  }
]
}

```

Vous pouvez associer cette politique aux IAM utilisateurs de votre compte. Si un utilisateur nommé `richard-roe` tente de consulter un AWS CodeStar projet, le projet doit être étiqueté `Owner=richard-roe` ou `owner=richard-roe`. Dans le cas contraire, l'utilisateur se voit refuser l'accès. La clé de condition d'étiquette `Owner` correspond à la fois à `Owner` et à `owner`, car les noms de clé de condition ne sont pas sensibles à la casse. Pour plus d'informations, voir [Éléments IAM JSON de politique : condition](#) dans le guide de IAM l'utilisateur.

AWS CodeStar mises à jour des politiques AWS gérées

Consultez les détails des mises à jour des politiques AWS gérées AWS CodeStar depuis que ce service a commencé à suivre ces modifications. Pour recevoir des alertes automatiques concernant les modifications apportées à cette page, abonnez-vous au RSS fil sur la page [Historique du AWS CodeStar document](#).

Modification	Description	Date
AWSCodeStarFullAccessPolitique — Mettre à jour la	La politique des rôles AWS CodeStar d'accès a été mise à jour. Le résultat de la	24 mars 2023

Modification	Description	Date
AWSCodeStarFullAccess politique	politique est le même, mais la formation du cloud nécessite un ListStacks complément DescribeStacks, ce qui est déjà nécessaire.	
AWSCodeStarService RolePolitique — Mettre à jour la AWSCodeStarServiceRole politique	<p>La politique relative au rôle de AWS CodeStar service a été mise à jour afin de corriger les actions redondantes figurant dans la déclaration de politique.</p> <p>La politique des rôles de service permet au AWS CodeStar service d'effectuer des actions en votre nom.</p>	23 septembre 2021
AWS CodeStar a commencé à suivre les modifications	AWS CodeStar a commencé à suivre les modifications apportées AWS à ses politiques gérées.	23 septembre 2021

Résolution des problèmes d'identité et d'accès liés à AWS CodeStar

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

Rubriques

- [Je ne suis pas autorisé à effectuer une action dans AWS CodeStar](#)
- [Je ne suis pas autorisé à effectuer iam : PassRole](#)
- [Je souhaite autoriser des personnes extérieures à mon AWS compte à accéder à mes AWS CodeStar ressources](#)

Je ne suis pas autorisé à effectuer une action dans AWS CodeStar

Si l'AWS Management Console indique que vous n'êtes pas autorisé à effectuer une action, contactez votre administrateur pour obtenir de l'aide. Votre administrateur vous a fourni vos informations d'identification de connexion.

L'exemple d'erreur suivant se produit lorsque l'utilisateur `mateojacksonIAMutilisateur` essaie d'utiliser la console pour afficher les détails d'un *widget* mais ne dispose pas d'autorisations `codestar:GetWidget`.

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

Dans ce cas, Mateo demande à son administrateur de mettre à jour ses politiques pour lui permettre d'accéder à la ressource *my-example-widget* à l'aide de l'action `codestar:GetWidget`.

Je ne suis pas autorisé à effectuer iam : PassRole

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

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

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

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

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

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

Je souhaite autoriser des personnes extérieures à mon AWS compte à accéder à mes AWS CodeStar ressources

Vous pouvez créer un rôle que les utilisateurs provenant d'autres comptes ou les personnes extérieures à votre organisation pourront utiliser pour accéder à vos ressources. Vous pouvez spécifier qui est autorisé à assumer le rôle. Pour les services qui prennent en charge les politiques basées sur les ressources ou les listes de contrôle d'accès (ACLs), vous pouvez utiliser ces politiques pour autoriser les utilisateurs à accéder à vos ressources.

Pour en savoir plus, consultez les éléments suivants :

- Pour savoir si ces fonctionnalités sont prises AWS CodeStar en charge, consultez [Comment AWS CodeStar fonctionne avec IAM](#).
- Pour savoir comment donner accès à vos ressources sur un site Comptes AWS qui vous appartient, consultez la section [Fournir l'accès à un IAM utilisateur dans un autre site Compte AWS que vous possédez](#) dans le Guide de IAM l'utilisateur.
- 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 IAM l'utilisateur.
- Pour savoir comment fournir un accès via la fédération d'identité, consultez la section [Fournir un accès aux utilisateurs authentifiés de manière externe \(fédération d'identité\)](#) dans le guide de l'IAMutilisateur.
- Pour connaître la différence entre l'utilisation de rôles et l'utilisation de politiques basées sur les ressources pour l'accès entre comptes, voir Accès aux [ressources entre comptes IAM dans le guide](#) de l'IAMutilisateur.

Journalisation des AWS CodeStar appels d'API avec AWS CloudTrail

AWS CodeStar est intégré à AWS CloudTrail un service qui fournit un enregistrement des actions entreprises par un utilisateur, un rôle ou un AWS service dans AWS CodeStar. CloudTrail capture tous les appels d'API AWS CodeStar sous forme d'événements. Les appels capturés incluent les appels depuis la console AWS CodeStar et les appels de code aux opérations d'API AWS CodeStar. Si vous créez un suivi, vous pouvez activer la diffusion continue des CloudTrail événements vers un compartiment S3, y compris les événements pour AWS CodeStar. Si vous ne configurez pas de

suivi, vous pouvez toujours consulter les événements les plus récents dans la CloudTrail console dans Historique des événements. À l'aide des informations collectées par CloudTrail, vous pouvez déterminer la demande qui a été faite AWS CodeStar, l'adresse IP à partir de laquelle la demande a été faite, qui a fait la demande, quand elle a été faite et d'autres détails.

Pour en savoir plus CloudTrail, consultez le [guide de AWS CloudTrail l'utilisateur](#).

AWS CodeStar Informations dans CloudTrail

CloudTrail est activé sur votre AWS compte lorsque vous le créez. Lorsqu'une activité se produit dans AWS CodeStar, cette activité est enregistrée dans un CloudTrail événement avec d'autres événements de AWS service dans l'historique des événements. Vous pouvez afficher, rechercher et télécharger les événements récents dans votre compte AWS. Pour plus d'informations, consultez la section [Affichage des événements à l'aide de l'historique des CloudTrail événements](#).

Pour enregistrer en continu les événements dans votre compte AWS, y compris les événements d'AWS CodeStar, créez un journal d'activité. Par défaut, lorsque vous créez un journal d'activité dans la console, il s'applique à toutes les régions AWS. Le journal d'activité consigne les événements de toutes les régions dans la partition AWS et livre les fichiers journaux dans le compartiment S3 de votre choix. Vous pouvez configurer d'autres AWS services pour analyser et agir de manière plus approfondie sur les données d'événements collectées dans CloudTrail les journaux. Pour en savoir plus, consultez les ressources suivantes :

- [Présentation de la création d'un journal d'activité](#)
- [CloudTrail Services et intégrations pris en charge](#)
- [Configuration des notifications Amazon SNS pour CloudTrail](#)
- [Réception de fichiers CloudTrail journaux de plusieurs régions](#) et [réception de fichiers CloudTrail journaux de plusieurs comptes](#)

Toutes les AWS CodeStar actions sont enregistrées CloudTrail et documentées dans la [référence de l'AWS CodeStar API](#). Par exemple, les appels aux `DescribeProjectUpdateProject`, et `AssociateTeamMember` les actions génèrent des entrées dans les fichiers CloudTrail journaux.

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

- Si la demande a été effectuée avec les autorisations utilisateur root ou IAM .

- Si la demande a été effectuée avec des autorisations de sécurité temporaires pour un rôle ou un utilisateur fédéré.
- Si la requête a été effectuée par un autre service AWS.

Pour plus d'informations, consultez la section [Élément `userIdentity` CloudTrail](#).

Présentation des entrées des fichiers journaux AWS CodeStar

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

L'exemple suivant montre une entrée de CloudTrail journal illustrant l'appel d'une `CreateProject` opération AWS CodeStar :

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROAJLIN20F3UBEXAMPLE:role-name",
    "arn": "arn:aws:sts::account-ID:assumed-role/role-name/role-session-name",
    "accountId": "account-ID",
    "accessKeyId": "ASIAJ44LFQS5XEXAMPLE",
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2017-06-04T23:56:57Z"
      },
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROAJLIN20F3UBEXAMPLE",
        "arn": "arn:aws:iam::account-ID:role/service-role/role-name",
        "accountId": "account-ID",
        "userName": "role-name"
      }
    },
    "invokedBy": "codestar.amazonaws.com"
  },
  "eventTime": "2017-06-04T23:56:57Z",
```

```
"eventSource": "codestar.amazonaws.com",
"eventName": "CreateProject",
"awsRegion": "region-ID",
"sourceIPAddress": "codestar.amazonaws.com",
"userAgent": "codestar.amazonaws.com",
"requestParameters": {
  "clientRequestToken": "arn:aws:cloudformation:region-ID:account-ID:stack/stack-name/additional-ID",
  "id": "project-ID",
  "stackId": "arn:aws:cloudformation:region-ID:account-ID:stack/stack-name/additional-ID",
  "description": "AWS CodeStar created project",
  "name": "project-name",
  "projectTemplateId": "arn:aws:codestar:region-ID::project-template/project-template-name"
},
"responseElements": {
  "projectTemplateId": "arn:aws:codestar:region-ID::project-template/project-template-name",
  "arn": "arn:aws:codestar:us-east-1:account-ID:project/project-ID",
  "clientRequestToken": "arn:aws:cloudformation:region-ID:account-ID:stack/stack-name/additional-ID",
  "id": "project-ID"
},
"requestID": "7d7556d0-4981-11e7-a3bc-dd5daEXAMPLE",
"eventID": "6b0d6e28-7a1e-4a73-981b-c8fdbEXAMPLE",
"eventType": "AwsApiCall",
"recipientAccountId": "account-ID"
}
```

Validation de la conformité pour AWS CodeStar

AWS CodeStar n'entre pas dans le champ d'application des programmes de conformité AWS.

Pour obtenir la liste des services AWS concernés par des programmes de conformité spécifiques, consultez [AWSServices in Scope by Compliance Program \(Services concernés par les programmes de conformité\)](#). Pour obtenir des informations générales, consultez [AWSCompliance Programs \(Programmes de conformité\)](#).

Vous pouvez télécharger les rapports de l'audit externe avec AWS Artifact. Pour plus d'informations, consultez [Downloading Reports \(Téléchargement des rapports\) dans AWS Artifact](#).

Résilience dans AWS CodeStar

L'infrastructure mondiale AWS s'articule autour 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 en savoir plus sur les régions AWS et zones de disponibilité , consultez [Infrastructure mondiale AWS](#).

Sécurité de l'infrastructure dans AWS CodeStar

En tant que service géré, AWS CodeStar il est protégé par la sécurité du réseau AWS mondial. Pour plus d'informations sur les services AWS de sécurité et sur la manière dont AWS l'infrastructure est protégée, consultez la section [Sécurité du AWS cloud](#). Pour concevoir votre AWS environnement en utilisant les meilleures pratiques en matière de sécurité de l'infrastructure, consultez la section [Protection de l'infrastructure](#) dans le cadre AWS bien architecturé du pilier de sécurité.

Vous utilisez API les appels AWS publiés pour accéder CodeStar via le réseau. Les clients doivent prendre en charge les éléments suivants :

- Sécurité de la couche de transport (TLS). Nous avons besoin de la TLS version 1.2 et recommandons la TLS version 1.3.
- Des suites de chiffrement parfaitement confidentielles (PFS) telles que (Ephemeral Diffie-Hellman) ou DHE ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). La plupart des systèmes modernes tels que Java 7 et les versions ultérieures prennent en charge ces modes.

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

Par défaut, AWS CodeStar n'isole pas le trafic de service. Les projets créés avec AWS CodeStar sont ouverts à l'Internet public, sauf si vous modifiez manuellement les paramètres d'accès via

AmazonEC2, API Gateway ou Elastic Beanstalk. Ceci est intentionnel. Vous pouvez modifier les paramètres d'accès dans AmazonEC2, API Gateway ou Elastic Beanstalk comme vous le souhaitez, notamment en empêchant tout accès à Internet.

AWS CodeStar ne prend pas en charge les VPC endpoints (AWS PrivateLink) par défaut, mais vous pouvez configurer ce support directement sur les ressources du projet.

Limites dans AWS CodeStar

Le tableau suivant décrit les limites appliquées dans AWS CodeStar. AWS CodeStar dépend d'autres services AWS pour les ressources de projet. Certaines de ces limites de service peuvent être modifiées. Pour plus d'informations sur les limites qui peuvent être modifiées, consultez [Limites de service AWS](#).

Nombre de projets	333 projets au maximum dans un compte AWS. La limite réelle varie en fonction du niveau de dépendance des autres services (par exemple, le nombre maximum de pipelines CodePipeline autorisés pour votre AWS compte).
Nombre de AWS CodeStar projets auxquels un utilisateur IAM peut appartenir	Maximum de 10 par utilisateur IAM individuel.
ID de projet	<p>Dans un compte AWS, les ID de projet doivent être uniques. Les ID de projet doivent comporter au moins 2 caractères et 15 caractères au maximum. Caractères autorisés :</p> <p>Lettres a à z inclus.</p> <p>Chiffres 0 à 9 inclus.</p> <p>Caractère spécial - (signe moins).</p> <p>Tous les autres caractères : lettres capitales, espaces, . (point), @ (arobase) ou _ (trait de soulignement) ne sont pas autorisés.</p>
Noms de projet	Les noms de projet ne peuvent pas comporter plus de 100 caractères et commencer ou se terminer par un espace vide.

Descriptions de projet	Toute combinaison de caractères comportant entre 0 et 1 024 caractères. Les descriptions de projet sont facultatives.
Membres de l'équipe dans un projet AWS CodeStar	100
Nom d'affichage dans un profil utilisateur	Toute combinaison de caractères comportant entre 1 et 100 caractères. Les noms complets doivent comporter au moins un caractère. Ce caractère ne peut pas être un espace. Les noms complets ne peuvent pas commencer ou se terminer par un espace.
Adresse e-mail dans un profil utilisateur	L'adresse e-mail doit contenir un @ (arobase) et se terminer par une extension de domaine valide.
Accès fédéré, accès au compte racine ou accès temporaire à AWS CodeStar	AWS CodeStar prend en charge les utilisateurs fédérés et l'utilisation d'informations d'identification d'accès temporaire. L'utilisation d'AWS CodeStar avec un compte racine n'est pas recommandée.
Rôles IAM	Un maximum de 5 120 caractères dans toute politique gérée attachée à un rôle IAM.

Résolution des problèmes AWS CodeStar

Les informations suivantes peuvent vous aider à résoudre les problèmes courants dans AWS CodeStar.

Rubriques

- [Échec de création d'un projet : un projet n'a pas été créé](#)
- [Création de projet : une erreur s'affiche lorsque j'essaie de modifier la configuration Amazon EC2 lors de la création d'un projet](#)
- [Suppression de projet : un AWS CodeStar projet a été supprimé, mais les ressources existent toujours](#)
- [Échec de la gestion de l'équipe : impossible d'ajouter un utilisateur IAM à une équipe dans un projet AWS CodeStar](#)
- [Échec d'accès : un utilisateur fédéré ne peut pas accéder à un projet AWS CodeStar](#)
- [Échec d'accès : un utilisateur fédéré ne peut pas accéder à un environnement ou en créer un AWS Cloud9](#)
- [Échec d'accès : un utilisateur fédéré peut créer un AWS CodeStar projet, mais ne peut pas afficher les ressources du projet](#)
- [Problème avec le rôle de service : le rôle de service n'a pas pu être créé](#)
- [Problème lié au rôle de service : le rôle de service n'est pas valide ou est manquant](#)
- [Problème lié au rôle du projet : les vérifications de l'état de AWS Elastic Beanstalk santé échouent pour certaines instances d'un AWS CodeStar projet](#)
- [Problème lié au rôle de projet : un rôle de projet n'est pas valide ou est manquant](#)
- [Extensions de projet : Impossible de se connecter à JIRA](#)
- [GitHub: Impossible d'accéder à l'historique des validations, aux problèmes ou au code d'un dépôt](#)
- [AWS CloudFormation : Création de la pile annulée en raison d'autorisations manquantes](#)
- [AWS CloudFormation n'est pas autorisé à exécuter le rôle d'exécution iam : PassRole on Lambda](#)
- [Impossible de créer la connexion pour un GitHub dépôt](#)

Échec de création d'un projet : un projet n'a pas été créé

Problème : lorsque vous essayez de créer un projet, un message s'affiche indiquant que la création a échoué.

Correctifs possibles : les motifs d'échec les plus courants sont les suivants :

- Un projet portant cet identifiant existe déjà dans votre AWS compte, peut-être dans une autre AWS région.
- L'utilisateur IAM auquel vous vous êtes connecté AWS Management Console ne dispose pas des autorisations requises pour créer un projet.
- Le rôle AWS CodeStar de service ne dispose pas d'une ou de plusieurs autorisations requises.
- Vous avez atteint la limite maximale pour une ou plusieurs ressources pour un projet (par exemple, la limite des politiques gérées par le client dans IAM, les compartiments Amazon S3 ou les pipelines inclus). CodePipeline

Avant de créer un projet, vérifiez que la `AWSCodeStarFullAccess` politique est appliquée à votre utilisateur IAM. Pour plus d'informations, consultez [AWSCodeStarFullAccess Politique](#).

Lorsque vous créez un projet, assurez-vous que l'ID est unique et répond aux exigences AWS CodeStar . Assurez-vous d'avoir coché la case J'AWS CodeStar aimerais avoir l'autorisation d'administrer les AWS ressources en votre nom.

Pour résoudre d'autres problèmes, ouvrez la AWS CloudFormation console, choisissez la pile correspondant au projet que vous avez essayé de créer, puis cliquez sur l'onglet Événements. Un projet peut avoir plusieurs piles. Les noms de piles commencent par `awscodestar-` et sont suivis de l'ID du projet. Les piles peuvent se trouver sous la vue de filtre Deleted (Supprimé). Passez en revue tous les messages d'échec dans les événements de pile et résolvez le problème répertorié comme étant la cause de ces échecs.

Création de projet : une erreur s'affiche lorsque j'essaie de modifier la configuration Amazon EC2 lors de la création d'un projet

Problème : lorsque vous modifiez les options de configuration d'Amazon EC2 lors de la création d'un projet, un message d'erreur ou une option grisée s'affiche et vous ne pouvez pas poursuivre la création du projet.

Correctifs possibles : les motifs les plus courants d'un message d'erreur sont les suivants :

- Le VPC du modèle de AWS CodeStar projet (soit le VPC par défaut, soit celui utilisé lors de la modification de la configuration Amazon EC2) possède une location d'instance dédiée, et le type

d'instance n'est pas pris en charge pour les instances dédiées. Choisissez un autre type d'instance ou un autre Amazon VPC.

- Aucun Amazon VPC n'est associé à votre AWS compte. Vous avez peut-être supprimé le VPC par défaut et n'en avez pas créé d'autres. Ouvrez la console Amazon VPC à l'[adresse https://console.aws.amazon.com/vpc/](https://console.aws.amazon.com/vpc/), choisissez Vos VPC et assurez-vous qu'au moins un VPC est configuré. Si tel n'est pas le cas, créez-en un. Pour plus d'informations, consultez la [présentation d'Amazon Virtual Private Cloud](#) dans le guide de démarrage Amazon VPC.
- L'Amazon VPC ne possède aucun sous-réseau. Choisissez un autre VPC ou créez un sous-réseau pour ce VPC. Pour plus d'informations, consultez [Principes de base des VPC et des sous-réseaux](#).

Suppression de projet : un AWS CodeStar projet a été supprimé, mais les ressources existent toujours

Problème : un AWS CodeStar projet a été supprimé, mais les ressources créées pour ce projet existent toujours. Par défaut, AWS CodeStar supprime les ressources du projet lorsque celui-ci est supprimé. Certaines ressources, telles que les compartiments Amazon S3, sont conservées même si l'utilisateur coche la case Supprimer les ressources, car les compartiments peuvent contenir des données.

Corrections possibles : ouvrez la [AWS CloudFormation console](#) et recherchez une ou plusieurs AWS CloudFormation piles utilisées pour créer le projet. Les noms de piles commencent par `awscodestar-` et sont suivis de l'ID du projet. Les piles peuvent se trouver sous la vue de filtre Deleted (Supprimé). Passez en revue les événements associés à la pile pour découvrir les ressources créées pour le projet. Ouvrez la console pour chacune de ces ressources dans la AWS région où vous avez créé le AWS CodeStar projet, puis supprimez manuellement les ressources.

Ressources de projet qui peuvent demeurer dans le projet :

- Un ou plusieurs compartiments de projet dans Amazon S3. Contrairement aux autres ressources de projet, les compartiments de projet dans Amazon S3 ne sont pas supprimés lorsque la case Supprimer les AWS ressources associées avec le AWS CodeStar projet est cochée.

Ouvrez la console Amazon S3 sur <https://console.aws.amazon.com/s3/>.

- Un référentiel source pour votre projet dans CodeCommit.

Ouvrez la CodeCommit console à l'[adresse https://console.aws.amazon.com/codecommit/](https://console.aws.amazon.com/codecommit/).

- Un pipeline pour votre projet en CodePipeline.

Ouvrez la CodePipeline console à l'[adresse https://console.aws.amazon.com/codepipeline/](https://console.aws.amazon.com/codepipeline/).

- Une application et les groupes de déploiement associés dans CodeDeploy.

Ouvrez la CodeDeploy console à l'[adresse https://console.aws.amazon.com/codedeploy/](https://console.aws.amazon.com/codedeploy/).

- Une application et les environnements associés dans AWS Elastic Beanstalk.

[Ouvrez la console Elastic Beanstalk à l'adresse https://console.aws.amazon.com/elasticbeanstalk/](https://console.aws.amazon.com/elasticbeanstalk/).

- Une fonction dans AWS Lambda.

Ouvrez la AWS Lambda console à l'[adresse https://console.aws.amazon.com/lambda/](https://console.aws.amazon.com/lambda/).

- Une ou plusieurs API dans API Gateway.

Ouvrez la console API Gateway à l'adresse <https://console.aws.amazon.com/apigateway/>.

- Une ou plusieurs politiques ou rôles IAM dans IAM.

Connectez-vous à la console IAM AWS Management Console et ouvrez-la à l'adresse <https://console.aws.amazon.com/iam/>.

- Une instance dans Amazon EC2.

Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.

- Un ou plusieurs environnements de développement dans AWS Cloud9.

Pour consulter, accéder et gérer les environnements de développement, ouvrez la AWS Cloud9 console à l'[adresse https://console.aws.amazon.com/cloud9/](https://console.aws.amazon.com/cloud9/).

Si votre projet utilise des ressources extérieures AWS (par exemple, un GitHub référentiel ou des problèmes dans Atlassian JIRA), ces ressources ne sont pas supprimées, même si la case Supprimer les AWS ressources associées avec le CodeStar projet est sélectionnée.

Échec de la gestion de l'équipe : impossible d'ajouter un utilisateur IAM à une équipe dans un projet AWS CodeStar

Problème : lorsque vous essayez d'ajouter un utilisateur à un projet, un message s'affiche indiquant que l'ajout a échoué.

Correctifs possibles : La raison la plus courante de cette erreur est que l'utilisateur a atteint le nombre limite de politiques gérées pouvant être appliquées à un utilisateur dans IAM. Vous pouvez

également recevoir cette erreur si vous n'avez pas le rôle de propriétaire dans le AWS CodeStar projet auquel vous avez essayé d'ajouter l'utilisateur, ou si l'utilisateur IAM n'existe pas ou a été supprimé.

Assurez-vous d'être connecté en tant qu'utilisateur propriétaire de ce AWS CodeStar projet. Pour plus d'informations, consultez [Ajouter des membres de l'équipe à un projet AWS CodeStar](#).

Pour résoudre d'autres problèmes, ouvrez la console IAM, choisissez l'utilisateur que vous avez essayé d'ajouter et vérifiez le nombre de politiques gérées appliquées à cet utilisateur IAM.

Pour plus d'informations, consultez [Limitations des entités et objets IAM](#). Pour plus d'informations sur les limites qui peuvent être modifiées, consultez [Limites de service AWS](#).

Échec d'accès : un utilisateur fédéré ne peut pas accéder à un projet AWS CodeStar

Problème : un utilisateur fédéré ne peut pas voir les projets dans la AWS CodeStar console.

Correctifs possibles : si vous êtes connecté en tant qu'utilisateur fédéré, assurez-vous de disposer de la stratégie gérée correcte attachée au rôle que vous assumez pour vous connecter. Pour plus d'informations, consultez [Associez la politique gérée par le AWS CodeStar visualiseur/contributeur/propriétaire de votre projet au rôle de l'utilisateur fédéré](#).

Ajoutez des utilisateurs fédérés à votre AWS Cloud9 environnement en attachant manuellement des politiques. veuillez consulter [Associer une politique AWS Cloud9 gérée au rôle de l'utilisateur fédéré](#).

Échec d'accès : un utilisateur fédéré ne peut pas accéder à un environnement ou en créer un AWS Cloud9

Problème : un utilisateur fédéré n'est pas en mesure de voir ou de créer un AWS Cloud9 environnement dans la AWS Cloud9 console.

Correctifs possibles : si vous êtes connecté en tant qu'utilisateur fédéré, assurez-vous de disposer de la stratégie gérée correcte attachée au rôle d'utilisateur fédéré.

Vous ajoutez des utilisateurs fédérés à votre AWS Cloud9 environnement en attachant manuellement des politiques au rôle de l'utilisateur fédéré. veuillez consulter [Associer une politique AWS Cloud9 gérée au rôle de l'utilisateur fédéré](#).

Échec d'accès : un utilisateur fédéré peut créer un AWS CodeStar projet, mais ne peut pas afficher les ressources du projet

Problème : un utilisateur fédéré a été en mesure de créer un projet, mais ne peut pas consulter les ressources du projet, telles que le pipeline du projet.

Corrections possibles : si vous avez joint la politique **AWSCodeStarFullAccess** gérée, vous êtes autorisé à créer un projet dans AWS CodeStar. Toutefois, pour accéder à toutes les ressources de projet, vous devez attacher la stratégie gérée de propriétaire.

Une fois AWS CodeStar les ressources du projet créées, les autorisations de projet pour toutes les ressources du projet sont disponibles dans les politiques gérées par le propriétaire, le contributeur et le lecteur. Pour accéder à toutes les ressources, vous devez attacher manuellement la stratégie de propriétaire à votre rôle. veuillez consulter [Étape 3 : Configurer les autorisations IAM de l'utilisateur](#).

Problème avec le rôle de service : le rôle de service n'a pas pu être créé

Problème : Lorsque vous essayez de créer un projet dans AWS CodeStar, un message vous invitant à créer le rôle de service s'affiche. Lorsque vous choisissez l'option pour le créer, une erreur s'affiche.

Corrections possibles : La raison la plus courante de cette erreur est que vous êtes connecté AWS à un compte qui ne dispose pas des autorisations suffisantes pour créer le rôle de service. Pour créer le rôle de AWS CodeStar service (`aws-codestar-service-role`), vous devez être connecté en tant qu'utilisateur administratif ou avec un compte root. Déconnectez-vous de la console, puis connectez-vous avec un utilisateur IAM auquel la politique `AdministratorAccess` gérée est appliquée.

Problème lié au rôle de service : le rôle de service n'est pas valide ou est manquant

Problème : Lorsque vous ouvrez la AWS CodeStar console, un message s'affiche indiquant que le rôle de AWS CodeStar service est manquant ou non valide.

Correctifs possibles : le plus souvent, cette erreur provient du fait qu'un utilisateur administratif a modifié ou supprimé le rôle de service (`aws-codestar-service-role`). Si le rôle de service a été supprimé, vous êtes invité à le créer. Pour créer ce rôle, vous devez être connecté en

tant qu'utilisateur administrateur ou avec un compte racine. Si le rôle a été modifié, il n'est plus valide. Connectez-vous à la console IAM en tant qu'utilisateur administratif, recherchez le rôle de service dans la liste des rôles, puis supprimez-le. Passez à la AWS CodeStar console et suivez les instructions pour créer le rôle de service.

Problème lié au rôle du projet : les vérifications de l'état de AWS Elastic Beanstalk santé échouent pour certaines instances d'un AWS CodeStar projet

Problème : si vous avez créé un AWS CodeStar projet incluant Elastic Beanstalk avant le 22 septembre 2017, les vérifications de l'état de santé d'Elastic Beanstalk risquent d'échouer. Si vous n'avez pas modifié la configuration d'Elastic Beanstalk depuis la création du projet, la vérification de l'état de santé échoue et indique un état gris. Malgré l'échec de vérification de l'état, votre application doit continuer à s'exécuter comme prévu. Si vous avez modifié la configuration d'Elastic Beanstalk depuis la création du projet, la vérification de l'état de santé échoue et votre application risque de ne pas fonctionner correctement.

Correctif : les déclarations de politique IAM requises sont manquantes dans un ou plusieurs rôles IAM. Ajoutez les stratégies manquantes aux rôles concernés dans votre compte AWS .

1. Connectez-vous à la console IAM AWS Management Console et ouvrez-la à l'adresse <https://console.aws.amazon.com/iam/>.
(Si vous ne pouvez pas le faire, contactez l'administrateur de votre AWS compte pour obtenir de l'aide.)
2. Dans le panneau de navigation, choisissez Roles (Rôles).
3. Dans la liste des rôles, choisissez CodeStarWorker- **Project-ID** -EB, où **Project-ID est l'ID** de l'un des projets concernés. (Si vous ne pouvez pas trouver facilement un rôle dans la liste, saisissez tout ou partie du nom du rôle dans la zone Recherche.)
4. Sous l'onglet Permissions, choisissez Attach Policy.
5. Dans la liste des politiques, sélectionnez AWSElasticBeanstalkEnhancedHealthet AWSElasticBeanstalkService. (Si vous ne pouvez pas trouver facilement une stratégie dans la liste, saisissez tout ou partie du nom de la stratégie dans la zone de recherche.)
6. Choisissez Attach Policy (Attacher une politique).
7. Répétez les étapes 3 à 6 pour chaque rôle concerné dont le nom suit le modèle CodeStarWorker- **Project-ID** -EB.

Problème lié au rôle de projet : un rôle de projet n'est pas valide ou est manquant

Problème : lorsque vous essayez d'ajouter un utilisateur à un projet, un message d'erreur s'affiche indiquant que l'ajout a échoué, car la stratégie correspondant à un rôle de projet est manquante ou non valide.

Corrections possibles : La raison la plus courante de cette erreur est qu'une ou plusieurs politiques de projet ont été modifiées ou supprimées dans IAM. Les politiques de projet sont propres aux AWS CodeStar projets et ne peuvent pas être recréées. Le projet ne peut pas être utilisé. Créez un projet dans AWS CodeStar, puis migrez les données vers le nouveau projet. Clonez le code de projet depuis le référentiel du projet inutilisable et envoyez ce code dans le référentiel du nouveau projet. Copiez les informations Wiki de l'équipe de l'ancien projet vers le nouveau projet. Ajoutez les utilisateurs au nouveau projet. Lorsque vous êtes sûr d'avoir migré toutes les données et tous les paramètres, supprimez le projet inutilisable.

Extensions de projet : Impossible de se connecter à JIRA

Problème : Lorsque vous utilisez l'extension Atlassian JIRA pour essayer de connecter un AWS CodeStar projet à une instance JIRA, le message suivant s'affiche : « L'URL n'est pas une URL JIRA valide. Verify that the URL is correct. »

Correctifs possibles :

- Vérifiez que l'URL JIRA est correcte, puis réessayez de vous connecter.
- Votre instance JIRA auto-hébergée est peut-être inaccessible via le réseau Internet public. Contactez votre administrateur réseau pour vérifier que votre instance JIRA est accessible via le réseau Internet public, puis réessayez de vous connecter.

GitHub: Impossible d'accéder à l'historique des validations, aux problèmes ou au code d'un dépôt

Problème : dans le tableau de bord d'un projet qui stocke son code GitHub, les vignettes Historique des validations et GitHubProblèmes affichent une erreur de connexion, ou le fait de choisir Ouvrir dans GitHub ou Créer un problème dans ces vignettes affiche une erreur.

Causes possibles :

- Le AWS CodeStar projet n'a peut-être plus accès au GitHub référentiel.
- Le référentiel a peut-être été supprimé ou renommé en GitHub.

AWS CloudFormation : Création de la pile annulée en raison d'autorisations manquantes

Après avoir ajouté une ressource au fichier `template.yml`, affichez la mise à jour de la pile AWS CloudFormation pour tous les messages d'erreur. La mise à jour de la pile échoue si certains critères ne sont pas satisfaits (par exemple, lorsque les autorisations d'accès à des ressources obligatoires sont manquantes).

Note

Depuis le 2 mai 2019, nous avons mis à jour la politique relative au rôle des AWS CloudFormation travailleurs pour tous les projets existants. Cette mise à jour diminue la portée des autorisations d'accès accordées à votre pipeline de projet pour améliorer la sécurité dans vos projets.

Pour résoudre le problème, consultez l'état de défaillance dans la vue du AWS CodeStar tableau de bord du pipeline de votre projet.

Ensuite, choisissez le CloudFormation lien dans la phase de déploiement de votre pipeline pour résoudre le problème de la AWS CloudFormation console. Pour afficher les détails de création de la pile, développez la liste Événements de votre projet et affichez tous les messages d'échec. Le message indique l'autorisation manquante. Corrigez la stratégie du rôle du travail AWS CloudFormation , puis exécutez votre pipeline à nouveau.

AWS CloudFormation n'est pas autorisé à exécuter le rôle d'exécution iam : PassRole on Lambda

Si vous avez un projet créé avant le 6 décembre 2018 PDT qui crée des fonctions Lambda, AWS CloudFormation une erreur comme celle-ci peut s'afficher :

```
User: arn:aws:sts::id:assumed-role/CodeStarWorker-project-id-CloudFormation/  
AWSCloudFormation is not authorized to perform: iam:PassRole on resource:
```

```
arn:aws:iam::id:role/CodeStarWorker-project-id-Lambda (Service: AWSLambdaInternal;  
Status Code: 403; Error Code: AccessDeniedException; Request ID: id)
```

Cette erreur se produit parce que votre rôle de AWS CloudFormation travailleur n'est pas autorisé à transmettre un rôle pour le provisionnement de votre nouvelle fonction Lambda.

Pour corriger cette erreur, vous devez mettre à jour votre politique de rôle de AWS CloudFormation travailleur avec l'extrait de code suivant.

```
{  
    "Action": [ "iam:PassRole" ],  
    "Resource": [  
        "arn:aws:iam::account-id:role/CodeStarWorker-project-id-Lambda",  
    ],  
    "Effect": "Allow"  
}
```

Une fois que vous avez mis à jour la stratégie, exécutez votre pipeline à nouveau.

Vous pouvez également utiliser un rôle personnalisé pour votre fonction Lambda en ajoutant une limite d'autorisations à votre projet, comme décrit dans [Ajouter une limite d'IAutorisations aux projets existants](#)

Impossible de créer la connexion pour un GitHub dépôt

Problème :

Étant donné qu'une connexion à un GitHub référentiel utilise le AWS connecteur pour GitHub, vous devez disposer des autorisations du propriétaire de l'organisation ou des autorisations d'administrateur sur le référentiel pour créer la connexion.

Corrections possibles : pour plus d'informations sur les niveaux d'autorisation pour un GitHub référentiel, consultez <https://docs.github.com/en/free-pro-team@latest/github/setting-up-and-managing-organizations-and-teams/organization-permission-levels-for-an>

Notes de mise à jour du guide de l'utilisateur AWS CodeStar

Le tableau ci-après décrit les modifications importantes dans chaque édition du Guide de l'utilisateur AWS CodeStar. Pour recevoir les notifications des mises à jour de cette documentation, abonnez-vous à un flux RSS.

Modification	Description	Date
Mise à jour des politiques d'accès	La politique des rôles AWS CodeStar d'accès a été mise à jour. Le résultat de la politique est le même, mais la formation du cloud nécessite un ListStacks complément DescribeStacks, ce qui est déjà nécessaire. Pour faire référence à la politique mise à jour, reportez-vous à la section AWSCodeStarFullAccess Politique .	24 mars 2023
Mises à jour de la politique des rôles	La politique des rôles de AWS CodeStar service a été mise à jour. Pour faire référence à la politique mise à jour, reportez-vous à la section AWSCodeStarServiceRole Politique .	23 septembre 2021
Utiliser une ressource de connexion pour les projets dotés d'un référentiel GitHub source	Lorsque vous utilisez la console pour créer un projet dans AWS CodeStar un GitHub référentiel, une ressource de connexion est utilisée pour gérer vos GitHub actions. Les connexions utilisent GitHub des applications, tandis que l' GitHub	27 avril 2021

autorisation précédente utilisait OAuth. Pour un didacticiel expliquant comment créer un projet utilisant une connexion à GitHub, voir [Tutoriel : créer un projet avec un référentiel GitHub source](#). Le didacticiel explique également comment créer, réviser et fusionner une pull request pour le référentiel des sources de votre projet.

[AWS CodeStar soutiens AWS Cloud9 dans la région de l'ouest des États-Unis \(Californie du Nord\)](#)

AWS CodeStar prend désormais en charge l'utilisation AWS Cloud9 dans la région de l'ouest des États-Unis (Californie du Nord). Pour plus d'informations, consultez [Configuration de Cloud9](#).

16 février 2021

[Mettre à jour la documentation pour refléter la nouvelle expérience de console](#)

Le 12 août 2020, le AWS CodeStar service est passé à une nouvelle expérience utilisateur dans la AWS console. Le guide de l'utilisateur a été mis à jour pour correspondre à la nouvelle expérience de la console.

12 août 2020

[AWS CodeStarles projets peuvent être créés avec la AWS CodeStar CLI](#)

Les projets AWS CodeStar peuvent être créés avec la commande CLI. AWS CodeStar crée votre projet et votre infrastructure à l'aide du code source et du modèle de chaîne d'outils que vous fournissez. Voir [Créer un projet dans AWS CodeStar \(AWSCLI\)](#).

24 octobre 2018

[Tous les modèles de AWS CodeStar projet incluent désormais un AWS CloudFormation fichier pour les mises à jour de l'infrastructure](#)

AWS CodeStar fonctionne avec AWS CloudFormation pour vous permettre d'utiliser du code pour créer des services et des serveurs de support ou des plateformes sans serveur dans le cloud. Le AWS CloudFormation fichier est désormais disponible pour tous les types de modèles de AWS CodeStar projet (modèles avec la plateforme de calcul Lambda, EC2 ou Elastic Beanstalk). Le fichier est stocké dans `template.yaml` dans votre référentiel source. Vous pouvez afficher et modifier le fichier pour ajouter des ressources à votre projet. Consultez [Modèles de projet](#).

3 août 2018

[Notifications de mise à jour du Guide de l'utilisateur AWS CodeStar désormais disponibles via RSS](#)

La version HTML du Guide de l'utilisateur AWS CodeStar prend désormais en charge un flux RSS des mises à jour qui sont documentées sur la page Notes de mise à jour de la documentation. Le flux RSS inclut les mises à jour effectuées après le 30 juin 2018. Les mises à jour annoncées précédemment sont toujours disponibles sur la page Notes de mise à jour de la documentation. Utilisez le bouton RSS dans le panneau du menu supérieur pour vous abonner au flux.

30 juin 2018

Le tableau ci-après décrit les modifications importantes apportées dans chaque version du Guide de l'utilisateur AWS CodeStar avant le 30 juin 2018.

Modification	Description	Date de modification
Le guide de AWS CodeStar l'utilisateur est désormais disponible sur GitHub	Ce guide est désormais disponible sur GitHub. Vous pouvez également l'utiliser GitHub pour envoyer des commentaires et des demandes de modification concernant le contenu de ce guide. Pour plus d'informations, cliquez sur l'icône Modifier sur dans la barre de navigation du guide ou consultez le aws-codestar-user-guide référentiel awsdocs/ sur le site Web. GitHub	le 22 février 2018
AWS CodeStar est désormais disponible en Asie-Pacifique (Séoul)	AWS CodeStar est désormais disponible dans la région Asie-Pacifique (Séoul). Pour de plus amples informations, veuillez consulter AWS CodeStar dans le Référence générale d'Amazon Web Services.	14 février 2018

Modification	Description	Date de modification
AWS CodeStar est désormais disponible en Asie-Pacifique (Tokyo) et au Canada (centre)	AWS CodeStar est désormais disponible dans les régions Asie-Pacifique (Tokyo) et Canada (centre). Pour de plus amples informations, veuillez consulter AWS CodeStar dans le Référence générale d'Amazon Web Services.	20 décembre 2017
AWS CodeStar prend désormais en charge AWS Cloud9	AWS CodeStar prend désormais en charge l'utilisation d'AWS Cloud9, un IDE en ligne basé sur un navigateur, pour travailler avec le code de projet. Pour plus d'informations, veuillez consulter Utiliser AWS Cloud9 avec AWS CodeStar . Pour obtenir la liste des AWS régions prises en charge, consultez le Référence générale d'Amazon Web Services.	30 novembre 2017
AWS CodeStar prend désormais en charge GitHub	AWS CodeStar prend désormais en charge le stockage du code du projet dans GitHub. Pour plus d'informations, consultez Création d'un projet .	12 octobre 2017
AWS CodeStar est désormais disponible dans l'ouest des États-Unis (Californie du Nord) et en Europe (Londres)	AWS CodeStar est désormais disponible dans les régions de l'ouest des États-Unis (Californie du Nord) et de l'Europe (Londres). Pour de plus amples informations, veuillez consulter AWS CodeStar dans le Référence générale d'Amazon Web Services.	17 août 2017
AWS CodeStar est désormais disponible en Asie-Pacifique (Sydney), Asie-Pacifique (Singapour) et en Europe (Francfort)	AWS CodeStar est désormais disponible dans les régions Asie-Pacifique (Sydney), Asie-Pacifique (Singapour) et Europe (Francfort). Pour de plus amples informations, veuillez consulter AWS CodeStar dans le Référence générale d'Amazon Web Services.	25 juillet 2017

Modification	Description	Date de modification
AWS CloudTrail prend désormais en charge AWS CodeStar	AWS CodeStar est désormais intégré à CloudTrail un service qui capture les appels d'API effectués par ou pour le compte de votre AWS compte et envoie les fichiers journaux AWS CodeStar dans un compartiment Amazon S3 que vous spécifiez. Pour plus d'informations, veuillez consulter Journalisation des AWS CodeStar appels d'API avec AWS CloudTrail .	14 juin 2017
Première version	Il s'agit de la première version du Guide de l'utilisateur AWS CodeStar.	19 avril 2017

Glossaire AWS

Pour connaître la terminologie la plus récente d'AWS, consultez le [Glossaire AWS](#) dans la Référence Glossaire AWS.