aws

ユーザーガイド

AWS CodeStar

AWS CodeStar: ユーザーガイド

Table of Contents

2024 年 7 月 31 日、Amazon Web Services (AWS) は AWS CodeStar プロジェクトの作成と表示のサポートを終了します。2024 年 7 月 31 日以降は、 AWS CodeStar コンソールにアクセスしたり、新しいプロジェクトを作成したりできなくなります。ただし、ソースリポジトリ AWS CodeStar、パイプライン、ビルドなど、 によって作成された AWS リソースは、この変更の影響を受けず、引き続き機能します。 AWS CodeStar 接続と AWS CodeStar 通知は、この中止の影響を受けません。

作業の追跡、コードの開発、アプリケーションのビルド、テスト、デプロイをご希望の場合、Amazon CodeCatalyst に、合理化された導入プロセスと、ソフトウェアプロジェクトを管理するための追加機能が用意されています。Amazon CodeCatalyst の機能と価格について詳しくは、リンク先をご覧ください。

翻訳は機械翻訳により提供されています。提供された翻訳内容と英語版の間で齟齬、不一致または矛盾がある場合、英語版が優先します。

とは AWS CodeStar

AWS CodeStar は、 でソフトウェア開発プロジェクトを作成、管理、および操作するためのクラウドベースのサービスです AWS。 AWS CodeStar プロジェクト AWS を使用して、 でアプリケーションを迅速に開発、構築、デプロイできます。 AWS CodeStar プロジェクトは、プロジェクト開発ツールチェーン AWS のサービスを作成して統合します。 AWS CodeStar プロジェクトテンプレートの選択に応じて、そのツールチェーンにはソース管理、ビルド、デプロイ、仮想サーバー、サーバーレスリソースなどが含まれます。 は、プロジェクトユーザー (チームメンバーと呼ばれる) に必要なアクセス許可 AWS CodeStar も管理します。 AWS CodeStar プロジェクトにチームメンバーとしてユーザーを追加することで、プロジェクト所有者は各チームメンバーにプロジェクトとそのリソースへの適切なアクセスを迅速かつ簡単に付与できます。

トピック

で何ができますか AWS CodeStar？

AWS CodeStar を使用すると、クラウドでアプリケーション開発をセットアップし、単一の一元化されたダッシュボードから開発を管理できます。具体的な内容は以下のとおりです：

- ウェブアプリケーション、ウェブサービスなどの テンプレートを使用して、 で新しいソフトウェアプロジェクトを数分 AWS で開始します。 AWS CodeStar には、さまざまなプロジェクトタイプとプログラミング言語のプロジェクトテンプレートが含まれています。 AWS CodeStar はセットアップを処理するため、すべてのプロジェクトリソースが連携するように設定されます。
- チームのプロジェクトアクセスを管理する: AWS CodeStar は、プロジェクトチームメンバーに、ツールやリソースにアクセスするために必要なロールを割り当てることができる一元化されたコンソールを提供します。これらのアクセス許可は、プロジェクトで使用されるすべての AWS サービスに自動的に適用されるため、複雑な IAM ポリシーを作成または管理する必要はありません。
- プロジェクトを 1 か所で視覚化、運用、共同作業できます。プロジェクト、ツールチェーン、重要なイベントの全体像を示すプロジェクトダッシュボード AWS CodeStar が含まれています。最新のコードコミットなどの最新のプロジェクトアクティビティをモニタリングし、コード変更のステータス、ビルド結果、およびデプロイをすべて同じウェブページから追跡できます。1 つのダッシュボードからプロジェクトの状況をモニタリングし、問題を精査できます。

- 必要なすべてのツールで反復処理をすばやく実行する: AWS CodeStar には、プロジェクトの統合開発ツールチェーンが含まれています。チームメンバーがコードをプッシュすると、変更が自動的にデプロイされます。課題追跡機能との統合により、チームメンバーは次に何をする必要があるかを把握することができます。チームと連携して、コードの配信のすべてのフェーズでより迅速かつ効率的に作業できます。

の開始方法 AWS CodeStar

の使用を開始するには AWS CodeStar :

1. AWS CodeStar 「」の手順に従って、 を使用する準備をしますAWS CodeStarのセットアップ。
2. の開始方法 AWS CodeStar チュートリアルの手順に従って AWS CodeStar 、 を試してください。
3. AWS CodeStar プロジェクトにチームメンバーを追加する のステップに従って、他のデベロッパーとプロジェクトを共有します。
4. で IDE を使用する AWS CodeStar のステップに従って、利用したい IDE を統合します。

AWS CodeStarのセットアップ

の使用を開始する前に AWS CodeStar、次のステップを完了する必要があります。

トピック

ステップ 1: アカウントを作成する

にサインアップする AWS アカウント

がない場合は AWS アカウント、次の手順を実行して作成します。

にサインアップするには AWS アカウント

1. https://portal.aws.amazon.com/billing/signup を開きます。
2. オンラインの手順に従います。

   サインアップ手順の一環として、通話呼び出しを受け取り、電話キーパッドで検証コードを入力するように求められます。

   にサインアップすると AWS アカウント、 AWS アカウントのルートユーザー が作成されます。ルートユーザーには、アカウントのすべての AWS のサービス とリソースへのアクセス権があります。セキュリティのベストプラクティスとして、ユーザーに管理アクセスを割り当て、ルートユーザーのみを使用してルートユーザーアクセスが必要なタスクを実行してください。

AWS サインアッププロセスが完了すると、 から確認メールが送信されます。https://aws.amazon.com/ の [マイアカウント] をクリックして、いつでもアカウントの現在のアクティビティを表示し、アカウントを管理することができます。

管理アクセスを持つユーザーを作成する

にサインアップしたら AWS アカウント、日常的なタスクにルートユーザーを使用しないように AWS アカウントのルートユーザー、 のセキュリティを確保し AWS IAM アイデンティティセンター、 を有効にして管理ユーザーを作成します。

を保護する AWS アカウントのルートユーザー

1. ルートユーザーを選択し、 AWS アカウント E メールアドレスを入力して、アカウント所有者AWS マネジメントコンソールとして にサインインします。次のページでパスワードを入力します。

   ルートユーザーを使用してサインインする方法については、AWS サインイン ユーザーガイドのルートユーザーとしてサインインするを参照してください。
2. ルートユーザーの多要素認証 (MFA) を有効にします。

   手順については、IAM ユーザーガイドの AWS アカウント 「ルートユーザー (コンソール) の仮想 MFA デバイスを有効にする」を参照してください。

管理アクセスを持つユーザーを作成する

1. IAM アイデンティティセンターを有効にします。

   手順については、「AWS IAM アイデンティティセンター ユーザーガイド」の「AWS IAM アイデンティティセンターの有効化」を参照してください。
2. IAM アイデンティティセンターで、ユーザーに管理アクセスを付与します。

   を ID ソース IAM アイデンティティセンターディレクトリ として使用する方法のチュートリアルについては、AWS IAM アイデンティティセンター 「 ユーザーガイド」の「デフォルトを使用してユーザーアクセスを設定する IAM アイデンティティセンターディレクトリ」を参照してください。

管理アクセス権を持つユーザーとしてサインインする

- IAM アイデンティティセンターのユーザーとしてサインインするには、IAM アイデンティティセンターのユーザーの作成時に E メールアドレスに送信されたサインイン URL を使用します。

  IAM Identity Center ユーザーを使用してサインインする方法については、AWS サインイン 「 ユーザーガイド」の AWS 「 アクセスポータルにサインインする」を参照してください。

追加のユーザーにアクセス権を割り当てる

1. IAM アイデンティティセンターで、最小特権のアクセス許可を適用するというベストプラクティスに従ったアクセス許可セットを作成します。

   手順については、「AWS IAM アイデンティティセンター ユーザーガイド」の「権限設定を作成する」を参照してください。

2. グループにユーザーを割り当て、そのグループにシングルサインオンアクセス権を割り当てます。

   手順については、「AWS IAM アイデンティティセンター ユーザーガイド」の「グループの結合」を参照してください。

ステップ 2: AWS CodeStar サービスロールを作成する

ユーザーに代わって AWS リソースを管理するアクセス AWS CodeStar 許可と IAM アクセス許可を付与するために使用されるサービスロールを作成します。サービスロールは一度作成するだけで済みます。

> **Important**
>
> このサービスロールを作成するには、 管理ユーザー (またはルートアカウント) としてサインインする必要があります。詳細については、「最初の IAM ユーザーとグループの作成」を参照してください。

1. AWS CodeStar コンソールを https://console.aws.amazon.com/codestar/://https://https://https://https://https
2. [Start project] (プロジェクトのスタート) を選択します。

   [Start project] (プロジェクトのスタート) が表示されず、プロジェクトリストページに誘導されている場合は、サービスロールが作成されています。

3. [Create service role] (サービスロールの作成) で、[Yes, create role] (はい、ロールを作成します) を選択します。
4. ウィザードを終了します。詳細については後程見ていきます。

ステップ 3: ユーザーの IAM アクセス許可を設定する

管理ユーザーに加えて、IAM ユーザー、フェデレーティッドユーザー、ルートユーザー、または引き受けたロール AWS CodeStar として を使用できます。IAM ユーザーとフェデレーティッドユーザーに対して何が AWS CodeStar できるかについては、「」を参照してくださいAWS CodeStar の IAM ロール。

IAM ユーザーを設定していない場合は、「IAM ユーザー」を参照してください。

アクセス権限を付与するにはユーザー、グループ、またはロールにアクセス許可を追加します。

- 以下のユーザーとグループ AWS IAM アイデンティティセンター：

  アクセス許可セットを作成します。「AWS IAM アイデンティティセンター ユーザーガイド」の「権限設定を作成する」の手順に従ってください。

- IAM 内で、ID プロバイダーによって管理されているユーザー:

  ID フェデレーションのロールを作成します。詳細については、「IAM ユーザーガイド」の「サードパーティー ID プロバイダー (フェデレーション) 用のロールの作成」を参照してください。

- IAM ユーザー:
  - ユーザーが担当できるロールを作成します。手順については、「IAM ユーザーガイド」の「IAM ユーザー用ロールの作成」を参照してください。
  - (お奨めできない方法) ポリシーをユーザーに直接アタッチするか、ユーザーをユーザーグループに追加する。詳細については「IAM ユーザーガイド」の「ユーザー (コンソール) へのアクセス権限の追加」を参照してください。

ステップ 4: AWS CodeStar プロジェクトの Amazon EC2 キーペアの作成

多くの AWS CodeStar プロジェクトでは、 AWS CodeDeploy または を使用して Amazon EC2 インスタンス AWS Elastic Beanstalk にコードをデプロイします。プロジェクトに関連付けられている Amazon EC2 インスタンスにアクセスするには、IAM ユーザーの Amazon EC2 キーペアを作成します。IAM ユーザーは、Amazon EC2 キーを作成して管理するアクセス許可を持っている必要があります (例：`ec2:CreateKeyPair` アクションと `ec2:ImportKeyPair` アクションのアクセス許可)。詳細については、「Amazon EC2 のキーペア」 を参照してください。

ステップ 5: AWS CodeStar コンソールを開く

にサインインし AWS マネジメントコンソール、 AWS CodeStar コンソールを https://console.aws.amazon.com/codestar/://www.com で開きます。

次のステップ

これで、セットアップが完了しました。の使用を開始するには AWS CodeStar、「」を参照してくださいの開始方法 AWS CodeStar。

の開始方法 AWS CodeStar

このチュートリアルでは、 AWS CodeStar を使用してウェブアプリケーションを作成します。このプロジェクトには、ソースリポジトリのサンプルコード、継続的なデプロイツールチェーン、および、プロジェクトを表示およびモニタリングできるプロジェクトダッシュボードが含まれています。

このステップでは、次のことを行います：

- でプロジェクトを作成します AWS CodeStar。
- プロジェクトを調査します。
- コード変更をコミットします。
- コードの変更が自動的にデプロイされるのを確認します。
- プロジェクトで作業する他の人を追加します。
- 不要になったプロジェクトリソースをクリーンアップします。

> **Note**
>
> まだ行っていない場合は、まず「AWS CodeStarのセットアップ」のステップ (例: ステップ 2: AWS CodeStar サービスロールを作成する) を完了します。IAM の管理者ユーザーであるアカウントを使用してサインインする必要があります。プロジェクトを作成するには、**AWSCodeStarFullAccess**ポリシーを持つ IAM ユーザー AWS マネジメントコンソール を使用して にサインインする必要があります。

トピック

- チュートリアル: AWS CodeStar を使用して でプロジェクトを作成する AWS CLI
- チュートリアル: AWS CodeStarで Alexa スキルプロジェクトを作成する
- チュートリアル:GitHub ソースリポジトリを使用してプロジェクトを作成する

ステップ 1: AWS CodeStar プロジェクトを作成する

このステップでは、ウェブアプリケーション用の JavaScript (Node.js) ソフトウェア開発プロジェクトを作成します。 AWS CodeStar プロジェクトテンプレートを使用してプロジェクトを作成します。

> **Note**
>
> このチュートリアルで使用する AWS CodeStar プロジェクトテンプレートでは、次のオプションを使用します。
>
> - [Application category] (アプリケーションカテゴリー) : ウェブアプリケーション
> - [Programming language] (プログラム言語) : Node.js
> - AWS サービス: Amazon EC2
>
> 他のオプションを選択した場合は、このチュートリアルに記載されている内容と一致しない場合があります。

でプロジェクトを作成するには AWS CodeStar

1. にサインインし AWS マネジメントコンソール、 AWS CodeStar コンソールを https://console.aws.amazon.com/codestar/:///www.com で開きます。

   プロジェクトとそのリソースを作成する AWS リージョンにサインインしていることを確認します。たとえば、米国東部 (オハイオ) でプロジェクトを作成するには、その AWS リージョンが選択されていることを確認してください。 AWS CodeStar が利用可能な AWS リージョンの詳細については、 AWS 全般のリファレンスの「リージョンとエンドポイント」を参照してください。
2. [AWS CodeStar] ページで、[プロジェクトの作成] を選択します。
3. 「プロジェクトテンプレートの選択」ページで、プロジェクトテンプレートのリストから AWS CodeStar プロジェクトタイプを選択します。フィルタバーを使用して選択を絞り込むことがで

きます。例えば、Amazon EC2 インスタンスにデプロイされる Node.js で記述されたウェブアプリケーションプロジェクトの場合は、[Web application] (ウェブアプリケーション)、[Node.js] の順に選択し、[Amazon EC2] チェックボックスをオンにします。次に、オプションのセットで使用可能なテンプレートから選択します。

詳細については、「AWS CodeStar プロジェクトテンプレート」を参照してください。

4. [Next (次へ)] を選択します。
5. [プロジェクト名] で、*My First Project* などのプロジェクト名を入力します。[Project ID] (プロジェクト ID) では、プロジェクトの ID はこのプロジェクト名から派生しますが、15 文字の制限があります。

   例えば、*My First Project* という名前のプロジェクトのデフォルト ID は *my-first-projec* です。このプロジェクト ID は、プロジェクトに関連付けられているすべてのリソースの名前のベースです。 AWS CodeStar は、このプロジェクト ID をコードリポジトリの URL の一部として使用するほか、IAM の関連するセキュリティアクセスロールとポリシーの名前にも使用します。プロジェクトの作成後、プロジェクト ID は変更できません。プロジェクトを作成する前にプロジェクト ID を編集するには、[Project ID] (プロジェクト ID) で、使用する ID を入力します。

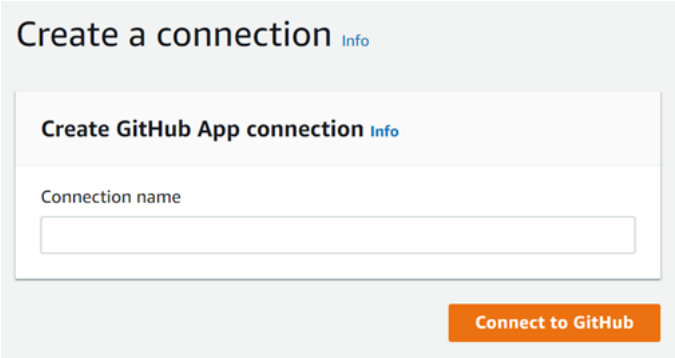
   プロジェクト名とプロジェクト ID の制限の詳細については、の制限 AWS CodeStar を参照してください。

   > **Note**
   >
   > プロジェクト IDsは、 AWS リージョンの AWS アカウントで一意である必要があります。

6. リポジトリプロバイダー、AWS CodeCommit または [GitHub] を選択します。
7. を選択した場合AWS CodeCommitは、リポジトリ名にデフォルトの AWS CodeCommit リポジトリ名を使用するか、別のリポジトリ名を入力します。ステップ 9 に進みます。
8. [GitHub] を選択した場合、接続リソースを選択または作成する必要があります。既存の接続がある場合は、検索フィールドで選択します。それ以外の場合は、ここで新しい接続を作成します。[Connect to GitHub] (GitHub に接続) を選択します。

   [Create a connection] (接続の作成) ページが表示されます。

> **Note**
>
> 接続を作成するには、GitHub アカウントが必要です。組織の接続を作成する場合は、組織の所有者である必要があります。



a. [GitHub App 接続の作成] で、[接続名] テキスト入力フィールドに接続名を入力します。[Connect to GitHub] (GitHub に接続) を選択します。

   [Connect to GitHub] (GitHub に接続) ページが表示され、[GitHub Apps] フィールドが表示されます。

b. [GitHub Apps] で、アプリケーションのインストールを選択するか、[Install a new app] (新しいアプリケーションをインストールする) を選択してアプリケーションを作成します。

   > **Note**
   >
   > 特定のプロバイダーへのすべての接続に対してアプリを 1 つインストールします。AWS Connector for GitHub アプリをすでにインストールしている場合は、それを選択してこのステップをスキップします。

c. 「Install AWS Connector for GitHub」ページで、アプリをインストールするアカウントを選択します。

> **Note**
>
> アプリケーションをインストール済みである場合は、[Configure] (設定) を選択してアプリのインストールの変更ページに進むか、戻るボタンでコンソールに戻ることができます。

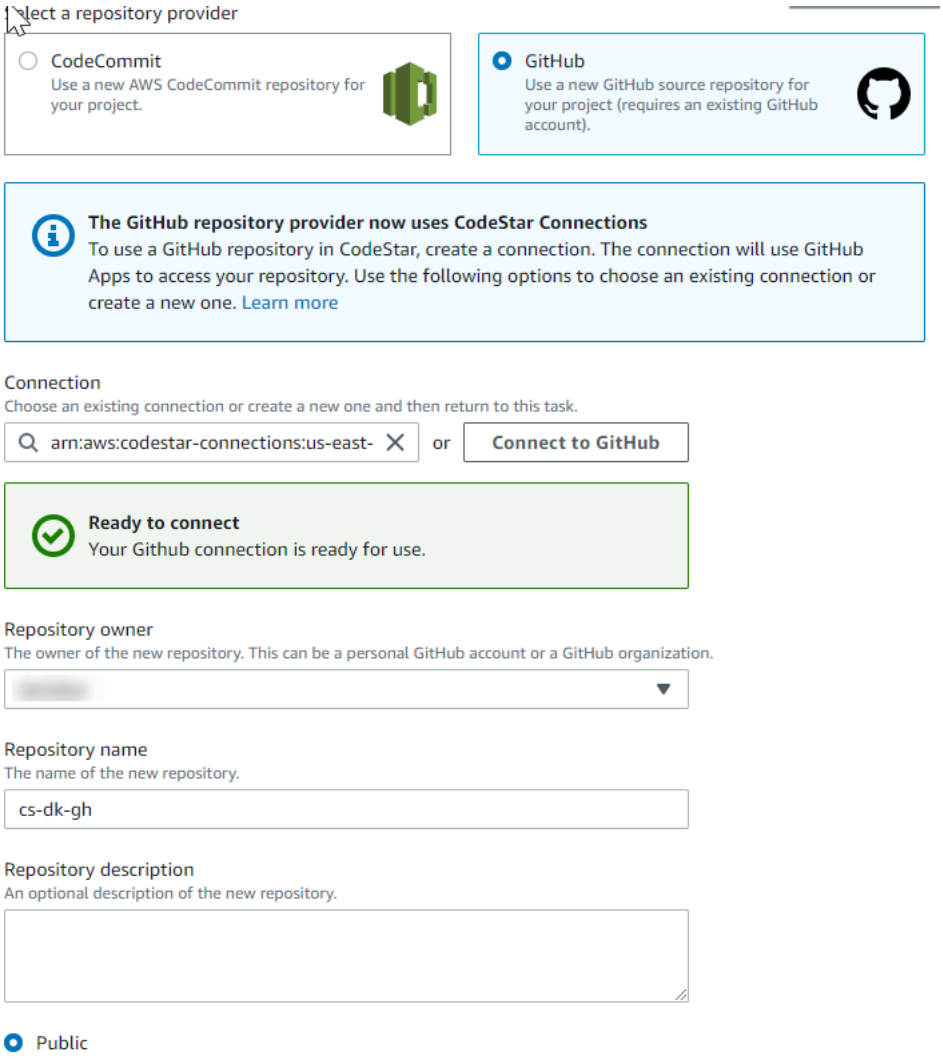
d. [Confirm password to continue] (パスワードを確認して続行) ページが表示される場合、GitHub パスワードを入力し、[Sign in] (サインイン) を選択します。

e. 「Install AWS Connector for GitHub」ページで、デフォルトのままにして、「Install」を選択します。

f. [GitHub へ接続] ページで、新規インストールのインストール ID が [GitHub Apps] テキスト入力フィールドに表示されます。

   接続が作成された後、CodeStar の [create project] (プロジェクトを作成) ページで、[Ready to connect] (接続準備完了) メッセージが表示されます。

> **Note**
>
> [Developer Tools] (デベロッパーツール) コンソールの[Settings] (設定) で接続を表示できます。詳細については、[Getting started with connections] (接続入門ガイド) を参照してください。



g. [Repository owner] (リポジトリ所有者) で、GitHub 組織または個人用 GitHub アカウントを選択します。

h. [Repository name] (リポジトリ名) で、デフォルトの GitHub リポジトリ名を受け入れるか、別の名前を入力します。

i. [Public] (公開) または[Private] (プライベート) を選択します。

> **Note**
>
> を開発環境 AWS Cloud9 として使用するには、Public を選択する必要があります。

j. (オプション) [Repository description] (リポジトリの説明) に、GitHub リポジトリの説明を入力します。

> **Note**
>
> Alexa スキルプロジェクトテンプレートを選択する場合は、Amazon 開発者アカウントを接続する必要があります。Alexa スキルプロジェクトの操作の詳細については、「チュートリアル: AWS CodeStarで Alexa スキルプロジェクトを作成する」を参照してください。

9. プロジェクトが Amazon EC2 インスタンスにデプロイされ、変更を加える場合は、[Amazon EC2 Configuration] (Amazon EC2 の設定) で Amazon EC2 インスタンスを設定します。例えば、プロジェクトの使用可能なインスタンスタイプから選択できます。

   > **Note**
   >
   > 異なる Amazon EC2 インスタンスタイプは、異なるレベルのコンピューティングパワーを提供し、異なる関連費用が発生する可能性があります。詳細については、[Amazon EC2 Instance Types] (Amazon EC2 インスタンスタイプ) と [Amazon EC2 Pricing] (Amazon EC2 の料金) を参照してください。
   > 複数の仮想プライベートクラウド (VPC) または複数のサブネットが Amazon 仮想プライベートクラウド で作成されている場合は、使用する VPC とサブネットを選択することもできます。ただし、ハードウェア専有インスタンスでサポートされていない Amazon EC2 インスタンスタイプを選択した場合は、インスタンスのテナンシーが [Dedicated] (専有) に設定されている VPC を選択することはできません。
   > 詳細については、[What Is Amazon VPC?] (Amazon VPC とは) および [Dedicated Instance Basics] (ハードウェア専有インスタンスの基礎) を参照してください。

   [Key pair] (キーペア) で、ステップ 4: AWS CodeStar プロジェクトの Amazon EC2 キーペアの作成 で作成した Amazon EC2 キーペアを選択します。[I acknowledge that I have access to the private key file] (私はプライベートキーファイルへのアクセス権があることを認めます) を選択します。

10. [Next] (次へ) を選択します。
11. リソースと設定の詳細を確認します。
12. [Next] (次へ) または [Create project] (プロジェクトの作成) を選択します。(表示される選択はプロジェクトテンプレートによって異なります。)

プロジェクト (リポジトリを含む) の作成には数分かかる場合があります。

13. プロジェクトのリポジトリの作成後は、[Repository] (リポジトリ) ページを使用して、リポジトリへのアクセス権を設定します。[Next steps] (次のステップ) のリンクを使用して、IDE を設定、課題追跡を設定、チームメンバーをプロジェクトに追加できます。

ステップ 2: AWS CodeStar ユーザープロファイルの表示情報を追加する

プロジェクトを作成すると、所有者としてプロジェクトチームに追加されます。を初めて使用する場合は AWS CodeStar、以下を提供するように求められます。

- 他のユーザーに表示する表示名。
- 他のユーザーに表示する E メールアドレス。

この情報はユーザー AWS CodeStar プロファイルで使用されます。ユーザープロファイルはプロジェクト固有ではありませんが、 AWS リージョンに限定されます。プロジェクトに属している各 AWS リージョンにユーザープロファイルを作成する必要があります。希望に応じて、プロファイルごとに異なる情報を含めることができます。

ユーザー名と E メールアドレスを入力し、[Next] (次へ) を選択します。

> **Note**
>
> このユーザー名と E メールアドレスは、 AWS CodeStar ユーザープロファイルで使用されます。プロジェクトで 以外のリソース AWS (GitHub リポジトリや Atlassian JIRA の問題など) を使用している場合、それらのリソースプロバイダーには、異なるユーザー名と E メールアドレスを持つ独自のユーザープロファイルがある可能性があります。詳細については、リソースプロバイダのドキュメントを参照してください。

ステップ 3: プロジェクトを表示する

AWS CodeStar プロジェクトページは、プロジェクトへの最新のコミット、継続的デリバリーパイプラインの状態、インスタンスのパフォーマンスなど、プロジェクトリソースのステータスをユーザーとチームが表示する場所です。これらのリソースの詳細については、ナビゲーションバーから対応するページを選択してください。

新しいプロジェクトでは、ナビゲーションバーには次のページが表示されます：

- [Overview] (概要) ページには、プロジェクトのアクティビティ、プロジェクトリソース、およびプロジェクトの README コンテンツに関する情報が表示されます。
- [IDE]ページでは、プロジェクトを統合開発環境 (IDE) に接続して、ソースコードの変更を修正、テスト、プッシュします。これには、GitHub と AWS CodeCommit リポジトリの両方IDEs を設定する手順と AWS Cloud9 、環境に関する情報が含まれています。
- [Repository] (リポジトリ) ページには、名前、プロバイダー、最終変更日時、クローン URL など、リポジトリの詳細が表示されます。また、最新のコミットに関する情報を表示し、プルリクエストを作成することもできます。
- [Pipeline] (パイプライン) ページには、パイプラインに関する CI/CD 情報が表示されます。名前、最新のアクション、ステータスなどのパイプラインの詳細を表示できます。パイプラインの履歴を表示し、変更をリリースできます。また、パイプラインの個々のステップのステータスを表示することもできます。
- モニタリングページには、プロジェクトの設定に応じて Amazon EC2 または AWS Lambda メトリクスが表示されます。たとえば、パイプライン内の AWS Elastic Beanstalk または CodeDeploy リソースによって にデプロイされた Amazon EC2 インスタンスの CPU 使用率が表示されます。を使用するプロジェクトでは AWS Lambda、Lambda 関数の呼び出しメトリクスとエラーメトリクスが表示されます。この情報は時間単位で表示されます。このチュートリアルで提案された AWS CodeStar プロジェクトテンプレートを使用した場合、アプリケーションが最初にそれらのインスタンスにデプロイされるにつれて、アクティビティが著しく急増します。モニタリングを更新してインスタンスヘルスの変化を表示すると、問題やより多くのリソースの必要などを識別するのに役立ちます。
- 問題ページは、 AWS CodeStar プロジェクトを Atlassian JIRA プロジェクトと統合するためのものです。このタイルを設定すると、お客様やプロジェクトチームはプロジェクトダッシュボードから JIRA の課題を追跡できます。

コンソールの左側のナビゲーションペインでは、[Project] (プロジェクト)、[Team] (チーム)、[Settings] (設定) ページを移動できます。

ステップ 4: 変更をコミットする

まず、プロジェクトに含まれていたサンプルアプリケーションを表示します。プロジェクトナビゲーションのどこからでも [View application] (アプリケーションの表示) を選択して、アプリケーションの外観を確認します。新しいウインドウまたはブラウザのタブに、サンプルウェブアプリケーションが表示されます。これは、 が AWS CodeStar 構築およびデプロイしたプロジェクトサンプルです。

コードを確認するには、ナビゲーションバーで [Repository] (リポジトリ) を選択します。[Repository name] (リポジトリ名) の下にあるリンクを選択すると、プロジェクトのリポジトリが新しいタブまたはウィンドウで開きます。リポジトリの readme ファイル (`README.md`) の内容を読み、それらのファイルの内容を参照します。

このステップでは、コードを変更してその変更をリポジトリにプッシュします。これにはいくつかの方法があります：

- プロジェクトのコードが CodeCommit または GitHub リポジトリに保存されている場合は、 AWS Cloud9 を使用してウェブブラウザからコードを直接操作することができます。ツールのインストールは必要ありません。詳細については、「プロジェクトの AWS Cloud9 環境を作成する」を参照してください。
- プロジェクトのコードが CodeCommit リポジトリに保存されていて、Visual Studio または Eclipse がインストールされている場合は、 AWS Toolkit for Visual Studio または AWS Toolkit for Eclipse を使用してコードに簡単に接続できます。詳細については、「で IDE を使用する AWS CodeStar」を参照してください。Visual Studio または Eclipse がない場合は、Git クライアントをインストールし、このステップの後のステップに従ってください。
- プロジェクトのコードが GitHub リポジトリに保存されている場合は、IDE のツールを使用して GitHub に接続することができます。
  - Visual Studio では、GitHub Extension for Visual Studio などのツールを使用することができます。詳細については、GitHub Extension for Visual Studio ウェブサイトの [Overview] (概要) ページ、および GitHub ウェブサイトの [Getting Started with GitHub for Visual Studio] (GitHub for Visual Studio 入門) を参照してください。
  - Eclipse の場合は、EGit for Eclipse などのツールを使用することができます。詳細については、EGit ウェブサイトの [EGit Documentation] (EGit ドキュメント) を参照してください。
  - その他の IDE については、IDE のドキュメントを参照してください。
- 他の種類のコードリポジトリについては、リポジトリプロバイダのドキュメントを参照してください。

次の手順では、サンプルの基本的な変更を行う方法について説明します。

変更をコミットするようコンピュータを設定するには (IAM ユーザー)

> **Note**
>
> この手順では、プロジェクトのコードが CodeCommit リポジトリに保存されていることを想定しています。他の種類のコードリポジトリについては、リポジトリプロバイダのドキュメ

ントを参照してください。次の手順「プロジェクトリポジトリのクローンを作成して変更するには」に進みます。
コードが CodeCommit に保存されていて、CodeCommit を既に使用している場合、または AWS CodeStar コンソールを使用してプロジェクト AWS Cloud9 の開発環境を作成している場合、それ以上の設定は必要ありません。次の手順「プロジェクトリポジトリのクローンを作成して変更するには」に進みます。

1. ローカルコンピュータに Git をインストールします。
2. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/iam/:// www.com」で IAM コンソールを開きます。

   CodeCommit の AWS CodeStar プロジェクトリポジトリへの接続に Git 認証情報を使用する IAM ユーザーとしてサインインします。
3. IAM コンソールのナビゲーションペインで [Users] (ユーザー) を選択し、ユーザーのリストから自分の IAM ユーザーを選択します。
4. [User details] (ユーザーの詳細) ページで、[Security Credentials] (認証情報) タブを選択し、[HTTPS Git credentials for CodeCommit] (CodeCommit の HTTPS Git 認証情報) で、[Generate] (生成) を選択します。

   > **Note**
   >
   > Git 認証情報として自身のサインイン認証情報を選択することはできません。詳細については、[Use Git Credentials and HTTPS with CodeCommit] (CodeCommit で Git 認証情報と HTTPS を使用する) を参照してください。
5. IAM が生成したサインイン認証情報をコピーします。[Show] (表示) を選択しこの情報をローカルコンピュータの安全なファイルにコピーして貼り付ける、または、[Download credentials] (認証情報をダウンロード) を選択してこの情報を .CSV ファイルとしてダウンロードします。CodeCommit に接続するには、この情報が必要です。

   認証情報を保存したら、[Close] を選択します。

> **Important**
>
> これは、サインイン認証情報を保存する唯一の機会です。パスワードを保存しないと、IAM コンソールからユーザー名をコピーすることはできますが、パスワードを参照することはできません。パスワードをリセットして保存する必要があります。

変更をコミットするようコンピュータを設定するには (フェデレーティッドユーザー)

コンソールを使用してリポジトリにファイルをアップロードするか、Git を使用してローカルコンピュータから接続することができます。フェデレーティッドアクセスを使用している場合は、以下のステップに従い、Git を使用して、ローカルコンピュータからリポジトリに接続してクローンを作成します。

> **Note**
>
> この手順では、プロジェクトのコードが CodeCommit リポジトリに保存されていることを想定しています。他の種類のコードリポジトリについては、リポジトリプロバイダのドキュメントを参照してください。次の手順「プロジェクトリポジトリのクローンを作成して変更するには」に進みます。

1. ローカルコンピュータに Git をインストールします。
2. をインストールします AWS CLI。
3. フェデレーティッドユーザー用の一時的セキュリティ認証情報を設定します。詳細については、[Temporary Access to CodeCommit Repositories] (CodeCommit リポジトリへの一時アクセス) を参照してください。一時認証情報は、次で構成されます：

   - AWS アクセスキー
   - AWS シークレットキー
   - セッショントークン

   一時的なセキュリティ認証情報の詳細については、「GetFederationToken のアクセス許可」を参照してください。
4. AWS CLI 認証情報ヘルパーを使用してリポジトリに接続します。詳細については、「Linux、macOS、または Unix で AWS CLI 認証情報ヘルパーを使用した CodeCommit

リポジトリへの HTTPS 接続のセットアップ手順」または「CLI 認証情報ヘルパーを使用した Windows で CodeCommit リポジトリへの HTTPS AWS 接続のセットアップ手順」を参照してください。

5. 次の例では、CodeCommit リポジトリに接続し、コミットをプッシュする方法を示します。

例: プロジェクトリポジトリのクローンを作成して変更するには

> **Note**
>
> この手順では、プロジェクトのコードリポジトリをコンピュータに複製し、プロジェクトの `index.html` ファイルを変更して、その変更をリモートリポジトリにプッシュする方法を説明します。この手順では、CodeCommit プロジェクトのコードが リポジトリに保存されていることと、コマンドラインから Git クライアントを使用していることを前提としています。他の種類のコードリポジトリまたはツールでリポジトリを複製し、ファイルを変更してコードをプッシュする方法については、プロバイダのドキュメントを参照してください。

1. AWS CodeStar コンソールを使用してプロジェクトの AWS Cloud9 開発環境を作成した場合は、開発環境を開き、この手順のステップ 3 に進みます。開発環境を開くには、「プロジェクトの AWS Cloud9 環境を開く」を参照してください。

   AWS CodeStar コンソールでプロジェクトを開き、ナビゲーションバーでリポジトリを選択します。[Clone URL] (URLのクローンを作成) で、CodeCommit 用に設定した接続タイプのプロトコルを選択して、リンクをコピーします。例えば、CodeCommit 用の Git 認証情報の設定の手順に従っている場合は、[HTTPS] を選択します。

2. ローカルコンピュータで、端末またはコマンドラインウィンドウを開き、一時ディレクトリにディレクトリを変更します。[git clone] コマンドを実行して、リポジトリのクローンをコンピュータに作成します。コピーしたリンクを貼り付けます。例えば、CodeCommit では HTTPS を使用します :

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

   初めて接続すると、リポジトリのサインイン認証情報の入力を求められます。CodeCommitでは、前の手順でダウンロードした Git サインイン認証情報を入力します。

3. コンピュータのクローンしたディレクトリに移動し、内容を参照します。

4. index.html ファイル (パブリックフォルダ内) を開き、ファイルを変更します。たとえば、<H2> タグの後に次のような段落を追加します：

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

ファイルを保存します。

5. 端末またはコマンドプロンプトで、変更したファイルを追加し、変更をコミットし、プッシュします。

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

6. [Repository] (リポジトリ) ページで、進行中の変更を表示します。そのリポジトリのコミット履歴が、コミットメッセージを含め、コミットで更新されているのを確認できます。[Pipeline] (パイプライン) ページでは、パイプラインがリポジトリへの変更を取得し、構築およびデプロイをスタートするのを確認できます。ウェブアプリケーションのデプロイ後、[View application] (アプリケーションの表示) を選択して変更内容を表示します。

> **Note**
>
> いずれかの [Pipeline](パイプライン) ステージで[Failed] (失敗しました) が表示される場合は、以下のトラブルシューティングのヘルプを参照してください：
>
> - [Source] (ソース) ステージの場合は、AWS CodeCommit ユーザーガイドのトラブルシューティング AWS CodeCommitを参照してください。
> - [Build] (ビルド) ステージの場合は、AWS CodeBuild ユーザーガイドのトラブルシューティング AWS CodeBuildを参照してください。
> - [Deploy] (デプロイ) ステージの場合は、AWS CloudFormation ユーザーガイドのトラブルシューティング AWS CloudFormationを参照してください。
> - その他の問題については、「トラブルシューティング AWS CodeStar」を参照してください。

ステップ 5: チームメンバーの追加

すべての AWS CodeStar プロジェクトには 3 つの AWS CodeStar ロールが設定されています。各ロールは、プロジェクトとそのリソースへの独自のレベルのアクセスを提供します。

- [Owner] (所有者) : チームメンバーの追加と削除、プロジェクトダッシュボードの変更、プロジェクトの削除を行うことができます。
- [Contributor] (寄稿者) : コードが CodeCommit に保存されている場合は、プロジェクトダッシュボードを変更してコードを投稿できますが、チームメンバーの追加や削除、プロジェクトの削除を行うことはできません。これは、 AWS CodeStar プロジェクトのほとんどのチームメンバーに選択する必要があるロールです。
- [Viewer] (閲覧者) : コードが CodeCommit に保存されている場合は、プロジェクトダッシュボード、プロジェクトコード、およびプロジェクトの状態を表示できますが、プロジェクトダッシュボードからタイルを移動、追加、または削除することはできません。

> **Important**
>
> プロジェクトで 以外のリソース AWS (GitHub リポジトリや Atlassian JIRA の問題など) を使用している場合、それらのリソースへのアクセスはリソースプロバイダーによって制御されます AWS CodeStar。詳細については、リソースプロバイダのドキュメントを参照してください。
>
> AWS CodeStar プロジェクトにアクセスできるユーザーは、 AWS CodeStar コンソールを使用して、 の外部にある AWS がプロジェクトに関連するリソースにアクセスできる場合があります。
>
> AWS CodeStar では、プロジェクトチームのメンバーがプロジェクトの関連する AWS Cloud9 開発環境に参加することはできません。チームメンバーによる共有環境への参加を許可するには、「プロジェクトチームメンバーと AWS Cloud9 環境を共有する」を参照してください。

チームとプロジェクトロールの詳細については、「AWS CodeStar Teams の使用」 を参照してください。

プロジェクトにチームメンバーを追加するには AWS CodeStar （ コンソール ）

1. AWS CodeStar コンソールを https://console.aws.amazon.com/codestar/://www.com で開きます。

2. ナビゲーションペインから、[Projects] (プロジェクト) を選択し、プロジェクトを選択します。
3. プロジェクトのサイドナビゲーションペインで、[Team] (チーム) を選択します。
4. [Team members] (チームメンバー) ページで、[Add team member] (チームメンバーの追加) を選択します。
5. [Choose user] (ユーザーを選択) で、次のいずれかを実行します：

   - 追加する人物の IAM ユーザーがすでに存在する場合は、その IAM ユーザーをリストから選択します。

     > **Note**
     >
     > 別の AWS CodeStar プロジェクトに既に追加されているユーザーは、既存の AWS CodeStar ユーザーリストに表示されます。

     プロジェクトロールで、このユーザーの AWS CodeStar ロール (所有者、寄稿者、または閲覧者) を選択します。これは AWS CodeStar プロジェクトレベルのロールで、プロジェクトの所有者によってのみ変更できます。IAM ユーザーに適用すると、ロールは AWS CodeStar プロジェクトリソースへのアクセスに必要なすべてのアクセス許可を提供します。コードが IAM の CodeCommit に保存されている場合の Git 認証情報の作成と管理に必要なポリシー、または IAM でユーザーの Amazon EC2 SSH キーをアップロードするのに必要なポリシーが適用されます。

     > **Important**
     >
     > 該当のユーザーとしてコンソールにサインインしていない限り、IAM ユーザーの表示名または E メール情報を入力または変更することはできません。詳細については、「AWS CodeStar ユーザープロファイルの表示情報を管理する」を参照してください。

     [Add team member] (チームメンバーの追加) を選択します。

   - プロジェクトに追加する人物の IAM ユーザーが存在しない場合は、[Create new IAM user] (新規 IAM ユーザーを作成) を選択します。新しい IAM ユーザーを作成できる IAM コンソールにリダイレクトされます。詳細については、IAM ユーザーガイドの「IAM ユーザーの作成」を参照してください。 IAM ユーザーを作成したら、 AWS CodeStar コンソールに戻り、ユーザーのリストを更新して、作成した IAM ユーザーをドロップダウンリストから選択します。

この新しいユーザーに適用する AWS CodeStar表示名、E メールアドレス、プロジェクトロールを入力し、チームメンバーの追加を選択します。

> **Note**
>
> 管理しやすいように、少なくとも 1 人のユーザーにプロジェクトの所有者ロールを割り当てます。

6. 新しいチームメンバーに、次の情報を送信します：

   - AWS CodeStar プロジェクトの接続情報。
   - ソースコードが CodeCommit に保存されている場合、ローカルコンピュータから CodeCommit リポジトリに [instructions for setting up access with Git credentials] (Git 認証情報でアクセスを設定する手順)。
   - AWS CodeStar ユーザープロファイルの使用 で説明されているように、ユーザーが表示名、E メールアドレス、公開 Amazon EC2 SSH キーを管理する方法についての情報。
   - ユーザーが AWS を使用するのは初めてで、そのユーザーのために IAM ユーザーを作成した場合のワンタイムパスワードと接続情報。このパスワードはユーザーの初回サインイン時に失効します。ユーザーは新しいパスワードを選択する必要があります。

ステップ 6: クリーンアップ

お疲れ様でした。チュートリアルを完了しました。このプロジェクトとそのリソースを引き続き使用しない場合は、 AWS アカウントへの継続的な料金が発生しないように削除する必要があります。

でプロジェクトを削除するには AWS CodeStar

1. AWS CodeStar コンソールを https://console.aws.amazon.com/codestar/://https://https://https://https://https://https
2. ナビゲーションペインで、[Projects] (プロジェクト) を選択します。
3. 削除するプロジェクトを選択して、[Delete] (削除) を選択します。

   または、プロジェクトを開き、コンソールの左側のナビゲーションペインから [Settings] (設定) を選択します。[Project details] (プロジェクトの詳細)ページで、[Delete project] (プロジェクトの削除) を選択します。

4. [Delete confirmation page] (削除の確認ページ) で、[delete] (削除) と入力します。プロジェクトリソースを削除する場合、[Delete resources] (リソースの削除) を選択したままにします。[Delete] (削除) を選択します。

   プロジェクトの削除には数分かかる場合があります。削除されると、プロジェクトは AWS CodeStar コンソールのプロジェクトのリストに表示されなくなります。

   > **Important**
   >
   > プロジェクトで 以外のリソース AWS (GitHub リポジトリや Atlassian JIRA の問題など) を使用している場合、チェックボックスをオンにしても、それらのリソースは削除されません。
   > IAM ユーザーではないロールに AWS CodeStar 管理ポリシーを手動でアタッチしている場合、プロジェクトを削除することはできません。プロジェクトの管理ポリシーをフェデレーティッドユーザーのロールに添付している場合は、プロジェクトを削除する前にポリシーをデタッチする必要があります。詳細については、「???」を参照してください。

ステップ 7: 本番稼働環境のプロジェクトの準備

プロジェクトを作成したら、コードを作成、テスト、およびデプロイすることができます。本番稼働環境でプロジェクトを管理するには、次の考慮事項を確認してください。

- 定期的にパッチを適用し、アプリケーションで使用される依存関係のセキュリティベストプラクティスを確認してください。詳細については、「AWS CodeStar リソースで使用するセキュリティのベストプラクティス」を参照してください。
- プロジェクトのプログラミング言語で提案された環境設定を定期的にモニタリングします。

次のステップ

以下に、学習に役立つその他のリソースをいくつか示します AWS CodeStar。

- チュートリアル: AWS CodeStarでサーバーレスプロジェクトを作成および管理する は、 でロジックを使用してウェブサービスを作成およびデプロイするプロジェクトを使用し AWS Lambda 、Amazon API Gateway の API で呼び出すことができます。

- AWS CodeStar プロジェクトテンプレート で、作成できる他の種類のプロジェクトについて説明します。
- 他のユーザーによるプロジェクトの参加を許可する方法については、「AWS CodeStar Teams の使用」を参照してください。

チュートリアル: AWS CodeStarでサーバーレスプロジェクトを作成および管理する

このチュートリアルでは、 AWS CodeStar を使用して、 AWS サーバーレスアプリケーションモデル (AWS SAM) を使用して、 でホストされているウェブサービスの AWS リソースを作成および管理するプロジェクトを作成します AWS Lambda。

AWS CodeStar は、 に依存する AWS SAM を使用して AWS CloudFormation、Amazon API Gateway APIs、 AWS Lambda 関数、Amazon DynamoDB テーブルなど、サポートされている AWS リソースを簡単に作成および管理できます。(このプロジェクトでは Amazon DynamoDB テーブルを使用しません)。

詳細については、GitHub のAWS 「サーバーレスアプリケーションモデル (AWS SAM)」を参照してください。

前提条件:「AWS CodeStarのセットアップ」の手順を完了すること。

> **Note**
>
> AWS アカウントには、 が使用する AWS サービスのコストなど、このチュートリアルに関連するコストが請求される場合があります AWS CodeStar。詳細については、「AWS CodeStar 料金」を参照してください。

トピック

概要

このチュートリアルでは、次の作業を行います：

1. AWS CodeStar を使用して、SAM AWS を使用して Python ベースのウェブサービスを構築およびデプロイするプロジェクトを作成します。このウェブサービスは でホスト AWS Lambda されており、Amazon API Gateway からアクセスできます。
2. プロジェクトの主なリソースは次のとおりです：
   - プロジェクトのソースコードが保存されている AWS CodeCommit リポジトリ。このソースコードには、ウェブサービスのロジックが含まれ、関連する AWS リソースが定義されます。
   - ソースコードの構築を自動化する AWS CodePipeline パイプライン。このパイプラインは AWS SAM を使用して、関数を作成して にデプロイし AWS Lambda、Amazon API Gateway で関連する API を作成し、API を関数に接続します。
   - デプロイ先の 関数 AWS Lambda。
   - Amazon API Gateway で作成される API。
3. ウェブサービスをテストして、 がウェブサービスを期待どおりに AWS CodeStar 構築してデプロイしたことを確認します。
4. プロジェクトのソースコードを使用するようにローカルワークステーションを設定します。
5. ローカルワークステーションを使用してプロジェクトのソースコードを変更します。関数をプロジェクトに追加し、変更をソースコードにプッシュすると、 AWS CodeStar はウェブサービスの再構築と再デプロイを行います。
6. ウェブサービスを再度テストして、 が想定どおりに AWS CodeStar 再構築および再デプロイされたことを確認します。
7. ローカルワークステーションを使用してユニットテストを作成し、手動テストの一部を自動化されたテストに置き換えます。ユニットテストをプッシュすると、 はウェブサービスを AWS CodeStar 再構築して再デプロイし、ユニットテストを実行します。
8. ユニットテストの結果を表示します。

9. プロジェクトをクリーンアップします。このステップは、このチュートリアルに関連するコストに対する AWS アカウントへの請求を回避するのに役立ちます。

ステップ 1: プロジェクトを作成する

このステップでは、 AWS CodeStar コンソールを使用してプロジェクトを作成します。

1. にサインイン AWS マネジメントコンソール し、 AWS CodeStar コンソールを開きます。https://https://console.aws.amazon.com/codestar/.

   > **Note**
   >
   > で作成または識別した IAM ユーザーに関連付けられた認証情報 AWS マネジメントコンソール を使用して、 にサインインする必要がありますAWS CodeStarのセットアップ。このユーザーには、**AWSCodeStarFullAccess** マネージドポリシーが添付されている必要があります。

2. プロジェクトとそのリソースを作成する AWS リージョンを選択します。

   AWS CodeStar が利用可能な AWS リージョンの詳細については、 AWS 全般のリファレンスの「リージョンとエンドポイント」を参照してください。

3. [Create project] (プロジェクトの作成) を選択します。
4. [Choose a project template] (プロジェクトのテンプレートを選択する) ページで、以下を選択します：

   - [Application type] (アプリケーションの種類) で、[Web service] (ウェブサービス) を選択します。
   - [Programming language] (プログラミング言語) で、[Python] を選択します。
   - AWS サービスで、AWS Lambdaを選択します。

5. 選択した内容が含まれているボックスを選択します。[Next] (次へ) を選択します。
6. [Project name] (プロジェクト名) に、プロジェクトの名前 (例: **My SAM Project**) を入力します。例とは異なる名前を使用した場合は、必ずこのチュートリアル全体でそれを使用してください。

   プロジェクト ID の場合、このプロジェクトの関連識別子 (my-sam-project など) AWS CodeStar を選択します。別のプロジェクト ID が表示された場合は、このチュートリアル全体でそれを使用してください。

[AWS CodeCommit] は選択されたままにし、[Repository name] (リポジトリ名) の値は変更しないでください。

7. [Next] (次へ) を選択します。
8. 設定を確認し、[Create Project] (プロジェクトの作成) を選択します。

   この AWS リージョン AWS CodeStar で を初めて使用する場合は、表示名と E メールに、IAM ユーザー AWS CodeStar に使用する表示名と E メールアドレスを入力します。[Next (次へ)] を選択します。
9. がプロジェクト AWS CodeStar を作成するまで待ちます。この処理には数分かかることがあります。更新時に[Project provisioned] (プロジェクトのプロビジョニング完了)バナー が表示されるまで次に進まないでください。

ステップ 2: プロジェクトリソースを調べる

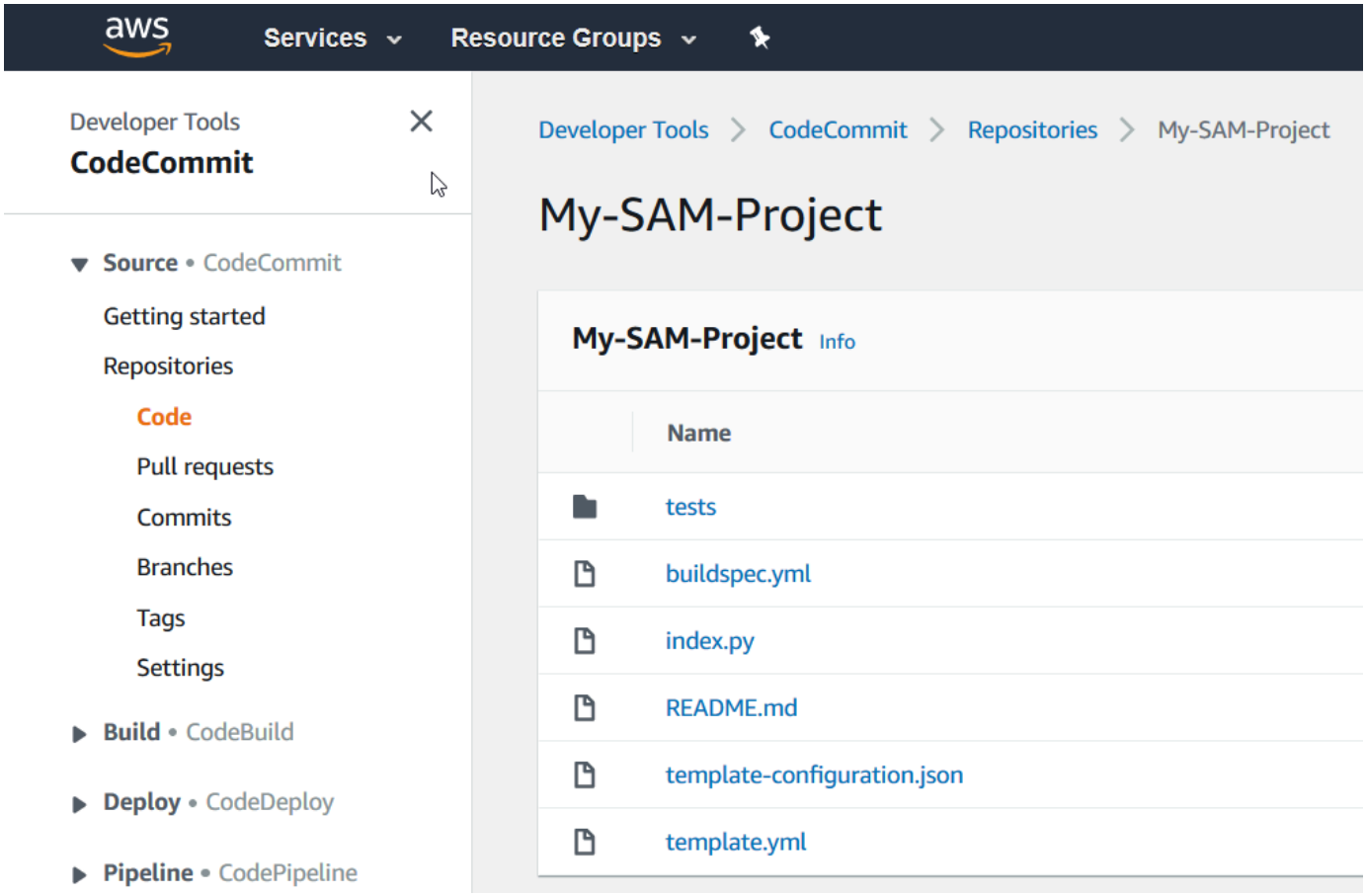
このステップでは、プロジェクトの 4 つの AWS リソースを調べて、プロジェクトの仕組みを理解します。

- プロジェクトのソースコードが保存されている AWS CodeCommit リポジトリ。 AWS CodeStar はリポジトリに my-sam-project という名前を付けます。my-sam-project はプロジェクトの名前です。
- CodeBuild と AWS SAM を使用して、API Gateway でのウェブサービスの Lambda 関数と API の構築とデプロイを自動化する AWS CodePipeline パイプライン。パイプラインには my-sam-project--Pipeline という名前 AWS CodeStar を付けます。my-sam-project はプロジェクトの ID です。
- ウェブサービスのロジックを含む Lambda 関数。 関数に awscodestar-my-sam-project-lambda-HelloWorld-*RANDOM_ID* という名前 AWS CodeStar を付けます。ここで、
  - [my-sam-project] はプロジェクトの ID です。
  - HelloWorld は、 AWS CodeCommit リポジトリの `template.yaml` ファイルで指定された関数 ID です。後でこのファイルについて説明します。
  - *RANDOM_ID* は、一意性を確保するために AWS SAM が関数に割り当てるランダム ID です。
- Lambda 関数の呼び出しを容易にする API Gateway の API。API に awscodestar-my-sam-project--lambda という名前 AWS CodeStar を付けます。my-sam-project はプロジェクトの ID です。

CodeCommit でソースコードリポジトリを確認するには

1. AWS CodeStar コンソールでプロジェクトを開き、ナビゲーションバーでリポジトリを選択します。
2. [Repository details] (リポジトリの詳細) で、CodeCommit リポジトリ (**My-SAM-Project**) へのリンクを選択します。
3. CodeCommit コンソールの [Code] (コード) ページに、プロジェクトのソースコードファイルが表示されます。

   - `buildspec.yml` では、CodePipeline が CodeBuild に対して、ビルドフェーズで AWS SAM を使用してウェブサービスをパッケージ化するように指示します。
   - `index.py` には、Lambda 関数のロジックが含まれています。この関数は、文字列「`Hello World`」と ISO 形式のタイムスタンプを出力します。
   - `README.md` には、リポジトリに関する一般的な情報が含まれています。
   - `template-configuration.json` には、プロジェクト ID でリソースにタグを付けるために使用されるプレースホルダ付きのプロジェクト ARN が含まれます。
   - `template.yml`。SAM AWS がウェブサービスをパッケージ化し、API Gateway で API を作成するために使用します。



ファイルの内容を表示するには、リストから選択します。

CodeCommit コンソール の使用の詳細については、「AWS CodeCommit ユーザーガイド」を参照してください。

CodePipeline でパイプラインを調べるには

1. パイプラインに関する情報を表示するには、 AWS CodeStar コンソールでプロジェクトを開き、ナビゲーションバーで [パイプライン] を選択します。パイプラインには以下が含まれています。

   - [Source] (ソース) は、CodeCommit からソースコードを取得するステージです。
   - [Build] (ビルド) は、CodeBuildでソースコードを構築するステージです。
   - AWS SAM を使用してビルドされたソースコードとリソースをデプロイするためのデプロイステージ。 AWS

2. パイプラインの詳細を表示するには、[Pipeline details] (パイプラインの詳細) で、パイプラインを選択して CodePipeline コンソールでパイプラインを開きます。

CodePipeline コンソールの使用の詳細については、「AWS CodePipeline ユーザーガイド」を参照してください。

概要ページでプロジェクトアクティビティと AWS サービスリソースを調べるには

1. AWS CodeStar コンソールでプロジェクトを開き、ナビゲーションバーから概要を選択します。
2. [Project activity] (プロジェクトアクティビティ) リストおよび [Project Resources] (プロジェクトリソース) リストを確認します。

Lambda で関数を調べるには

1. AWS CodeStar コンソールでプロジェクトを開き、サイドナビゲーションバーで概要を選択します。
2. [Project resources] (プロジェクトリソース) の [ARN]列で、Lambda 関数のリンクを選択します。

   関数のコードが Lambda コンソールに表示されます。

Lambda コンソールの使用の詳細については、「AWS Lambda デベロッパーガイド」を参照してください。

API Gateway で API を調べるには

1. AWS CodeStar コンソールでプロジェクトを開き、サイドナビゲーションバーで概要を選択します。
2. [Project resources] (プロジェクトリソース) の [ARN]列で、Amazon API Gateway API のリンクを選択します。

   API Gateway コンソールに API のリソースが表示されます。

API Gateway コンソールの使用については、API Gateway デベロッパーガイド を参照してください。

ステップ 3: ウェブサービスをテストする

このステップでは、構築してデプロイした AWS CodeStar ばかりのウェブサービスをテストします。

1. 前のステップからのプロジェクトを開いたままで、ナビゲーションバーの [Pipeline] (パイプライン) を選択します。
2. 続行する前に、[Source] (ソース)、[Build] (ビルド)、[Deploy] (デプロイ) ステージで、[Succeeded] (正常に完了) が表示されていることを確認します。この処理には数分かかることがあります。

   > **Note**
   >
   > いずれかのステージで [Failed] (失敗) が表示される場合は、以下のトラブルシューティングのヘルプを参照してください。
   >
   > - [Source] (ソース) ステージの場合は、AWS CodeCommit ユーザーガイドのトラブルシューティング AWS CodeCommitを参照してください。
   > - [Build] (ビルド) ステージの場合は、AWS CodeBuild ユーザーガイドのトラブルシューティング AWS CodeBuildを参照してください。
   > - [Deploy] (デプロイ) ステージの場合は、AWS CloudFormation ユーザーガイドのトラブルシューティング AWS CloudFormationを参照してください。
   > - その他の問題については、「トラブルシューティング AWS CodeStar」を参照してください。

3. [View Application] (アプリケーションの表示) を選択します。

ウェブブラウザで開いている新しいタブで、ウェブサービスは以下のレスポンス出力を表示します：

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

ステップ 4: プロジェクトコードを編集するためのローカルワークステーションの設定

このステップでは、ローカルワークステーションを設定して、AWS CodeStar プロジェクトのソースコードを編集します。ローカルワークステーションとして、macOS、Windows、または Linux を実行している物理コンピュータまたは仮想コンピュータを利用できます。

1. 前の手順でプロジェクトを開いたままにしておきます。

   - ナビゲーションバーで、[IDE] を選択し、[Access your project code] (プロジェクトコードにアクセス) を展開します。
   - [Command line interface] (コマンドラインインターフェイス) のしたの [View instructions] (手順の表示) を選択します。

     Visual Studio または Eclipse がインストールされている場合は、代わりに [Visual Studio] または [Eclipse] の下の [View instructions] (手順の表示) を選択し、手順に従って ステップ 5: ウェブサービスにロジックを追加する に進んでください。
2. 手順に従って、次のタスクを完了します：

   a. ローカルワークステーションに Git をセットアップします。
   b. IAM コンソールを使用して IAM ユーザーのための Git 認証情報を生成します。
   c. ローカルワークステーションにプロジェクトの CodeCommit リポジトリのクローンを作成します。
3. 左のナビゲーションで、[Project] (プロジェクト) を選択し、プロジェクトの概要に戻ります。

ステップ 5: ウェブサービスにロジックを追加する

このステップでは、ローカルワークステーションを使用してロジックをウェブサービスに追加します。具体的には、Lambda 関数を追加して API Gateway の API に接続します。

1. ローカルワークステーションで、クローンされたソースコードリポジトリが保存されているディレクトリに移動します。
2. そのディレクトリに `hello.py` という名前のファイルを作成します。次のコードを追加し、ファイルを保存します：

```
import json
```

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

上記のコードは、Hello という文字列と、呼び出し元が関数に送る文字列を出力します。

3. 同じディレクトリで template.yml ファイルを開きます。次のコードをファイルの末尾に追加し、ファイルを保存します。

```
  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
```

AWS SAM はこのコードを使用して Lambda で関数を作成し、API Gateway で API に新しいメソッドとパスを追加し、このメソッドとパスを新しい関数に接続します。

> **Note**
>
> 前述のコードのインデントは重要です。示されているように、コードを正確に追加しないと、プロジェクトが正しく構築されないことがあります。

4. git add . コマンドを実行して、ファイルの変更を複製されたリポジトリのステージングエリアに追加します。ピリオド (.) を忘れないでください。変更されたすべてのファイルに追加されます。

> **Note**
>
> コマンドラインの代わりに Visual Studio または Eclipse を使用している場合は、Git の使用方法が異なる場合があります。Visual Studio または Eclipse のドキュメントを参照してください。

5. git commit -m "Added hello.py and updated template.yaml." を実行して、クローンされたレポジトリのステージファイルをコミットします。
6. git push を実行してコミットをリモートリポジトリにプッシュします。

> **Note**
>
> 以前に生成したサインイン認証情報の入力を求めるメッセージが表示されることがあります。リモートリポジトリで作業するたびにこれが表示されることを防止するため、Git 認証情報マネージャーをインストールして設定することを考慮してみてください。例えば、macOS または Linux では、ターミナルで git config credential.helper 'cache --timeout 900' を実行して、15 分ごとにプロンプトを表示させることができます。または、git config credential.helper 'store --file ~/.git-credentials' を実行して、プロンプトを再度表示させないようにすることができます。Git は、認証情報をプレーンなファイルのクリアテキストとしてホームディレクトリに保存します。詳細については、Git ウェブサイトの [Git Tools - Credential Storage] (Git Tools - 認証情報ストレージ) を参照してください。

がプッシュ AWS CodeStar を検出すると、CodePipeline に CodeBuild と AWS SAM を使用してウェブサービスを再構築および再デプロイするよう指示します。[Pipeline] (パイプライン) ページで、デプロイの進行状況を確認できます。

AWS SAM は新しい関数に awscodestar-my-sam-project-lambda-Hello-***RANDOM_ID*** という名前を付けます。ここで、

- [my-sam-project] はプロジェクトの ID です。
- [Hello] は、`template.yaml` ファイルで指定された関数の ID です。

- *RANDOM_ID* は、SAM AWS が一意性のために関数に割り当てるランダム ID です。

ステップ 6: 拡張ウェブサービスをテストする

このステップでは、前のステップで追加したロジックに基づいて、 AWS CodeStar 構築およびデプロイされた拡張ウェブサービスをテストします。

1. プロジェクトを AWS CodeStar コンソールで開いたまま、ナビゲーションバーでパイプラインを選択します。
2. 続行する前に、パイプラインが再度実行されており、[Source] (ソース)、[Build] (ビルド)、[Deploy] (デプロイ) ステージで、[Succeeded] (正常に完了) が表示されていることを確認します。この処理には数分かかることがあります。

   > **Note**
   >
   > いずれかのステージで [Failed] (失敗) が表示される場合は、以下のトラブルシューティングのヘルプを参照してください。
   >
   > - [Source] (ソース) ステージの場合は、AWS CodeCommit ユーザーガイドのトラブルシューティング AWS CodeCommitを参照してください。
   > - [Build] (ビルド) ステージの場合は、AWS CodeBuild ユーザーガイドのトラブルシューティング AWS CodeBuildを参照してください。
   > - [Deploy] (デプロイ) ステージの場合は、AWS CloudFormation ユーザーガイドのトラブルシューティング AWS CloudFormationを参照してください。
   > - その他の問題については、「トラブルシューティング AWS CodeStar」を参照してください。

3. [View Application] (アプリケーションの表示) を選択します。

   ウェブブラウザで開いている新しいタブで、ウェブサービスは以下のレスポンス出力を表示します：

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

4. タブのアドレスボックスで、パス **/hello/** とファーストネームを URL の最後に追加 (例: https://***API_ID***.execute-api.***REGION_ID***.amazonaws.com/Prod/hello/***YOUR_FIRST_NAME***) し、[Enter] (入力) を押します。

ファーストネームが Mary の場合、ウェブサービスは、次のレスポンス出力を表示します :

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

ステップ 7: ウェブサービスにユニットテストを追加する

このステップでは、ローカルワークステーションを使用して、ウェブサービスで AWS CodeStar 実行されるテストを追加します。このテストは、以前に行った手動テストに代わるものです。

1. ローカルワークステーションで、クローンされたソースコードリポジトリが保存されているディレクトリに移動します。
2. そのディレクトリに hello_test.py という名前のファイルを作成します。次のコードを追加し、ファイルを保存します。

```
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
```

このテストは、Lambda 関数の出力が予想通りの形式であるかどうかをチェックします。予想通りの形式の場合、テストは成功です。そうでない場合は失敗です。

3. 同じディレクトリで buildspec.yml ファイルを開きます。ファイルの内容を次のコードに置き換えて、ファイルを保存します。

```
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
```

このビルド仕様では、CodeBuild に対して、ビルド環境に Python テストフレームワーク pytest をインストールするように指示します。CodeBuild は pytest を使用してユニットテストを実行します。これ以外のビルド仕様は、前に作成したものと同じです。

4. Git を使用して、これらの変更内容をリモートリポジトリにプッシュします。

```
git add .

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

git push
```

ステップ 8: ユニットテストの結果を表示する

このステップでは、ユニットテストが成功したか失敗したかを確認します。

1. プロジェクトを AWS CodeStar コンソールで開いたまま、ナビゲーションバーでパイプラインを選択します。
2. 続行する前に、パイプラインが再度実行されたことを確認します。この処理には数分かかることがあります。

   ユニットテストが成功した場合は、[Build] (ビルド) ステージに [Succeeded] (正常に終了) が表示されます。
3. ユニットテスト結果の詳細を表示するには、[Build] (ビルド) ステージで、 [CodeBuild] リンクを選択します。
4. CodeBuild コンソールの [Build Project: my-sam-project] ページの [Build history] (ビルド履歴) で、テーブルの [Build run] (ビルド実行) 列のリンクを選択します。
5. my-sam-project:***BUILD_ID*** ページの [Build logs] (ビルドログ) で、[View entire log] (全てのログを表示) リンクを選択します。
6. Amazon CloudWatch Logs コンソールに、次の例のようなテスト結果のログ出力が表示されます。次のテスト結果では、テストは成功しています。

```
...
============================= 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 ============================
...
```

テストが失敗した場合は、ログ出力に詳細が表示され、障害のトラブルシューティングに役立ちます。

ステップ 9: クリーンアップ

このステップでは、プロジェクトをクリーンアップして、このプロジェクトに継続的な料金が発生するのを回避します。

このプロジェクトを引き続き使用する場合は、このステップをスキップできますが、 AWS アカウントが引き続き課金される可能性があります。

1. プロジェクトを AWS CodeStar コンソールで開いたまま、ナビゲーションバーで設定を選択します。
2. [Project details] (プロジェクトの詳細) で、[Delete project] (プロジェクトの削除) を選択します。
3. **`delete`** を入力し、[Delete resources] (リソースの削除) ボックスをオンのまま、[Delete] (削除) を選択します。

> **Important**
>
> このボックスをオフにすると、プロジェクトレコードは から削除されますが AWS CodeStar、プロジェクトの AWS リソースの多くは保持されます。 AWS アカウントは引き続き課金される場合があります。

このプロジェクト用に が AWS CodeStar 作成した Amazon S3 バケットがまだある場合は、次のステップに従って削除します。

1. https://console.aws.amazon.com/s3/ で Amazon S3 コンソールを開きます。
2. バケットのリストで、[aws-codestar-***REGION_ID***-***ACCOUNT_ID***-my-sam-project--pipe] の横にあるアイコンを選択します。それぞれの種類の意味は次の通りです。

- *REGION_ID* は、先ほど削除したプロジェクトの AWS リージョンの ID です。
- *ACCOUNT_ID* は AWS アカウント ID です。
- [my-sam-project] は、今削除したプロジェクトの ID です。

3. [Empty Bucket] (バケットを空にする) を選択します。バケットの名前を入力し、[Confirm] (確認) を選択します。
4. [Delete Bucket] (バケットの削除) を選択します。バケットの名前を入力し、[Confirm] (確認) を選択します。

次のステップ

このチュートリアルを完了したら、次のリソースを確認することをお勧めします。

- の開始方法 AWS CodeStar チュートリアルでは、Amazon EC2 インスタンス上で実行されている Node.js ベースのウェブアプリケーションを作成しデプロイするプロジェクトを使用します。
- AWS CodeStar プロジェクトテンプレート で、作成できる他の種類のプロジェクトについて説明します。
- AWS CodeStar Teams の使用 では、他の人がどのようにプロジェクトに協力できるかを説明しています。

チュートリアル: AWS CodeStar を使用して でプロジェクトを作成する AWS CLI

このチュートリアルでは、 AWS CLI を使用して、サンプルソースコードとサンプルツールチェーンテンプレートを含む AWS CodeStar プロジェクトを作成する方法を示します。 は、 CloudFormation ツールチェーンテンプレートで指定された AWS インフラストラクチャと IAM リソースを AWS CodeStar プロビジョニングします。このプロジェクトでは、ツールチェーンのリソースを管理して、ソースコードの構築とデプロイを行います。

AWS CodeStar は CloudFormation を使用してサンプルコードを構築およびデプロイします。このサンプルコードは、 でホスト AWS Lambda され、Amazon API Gateway からアクセスできるウェブサービスを作成します。

前提条件:

- 「AWS CodeStarのセットアップ」のステップを完了します。

- Amazon S3 ストレージバケットを作成済みである必要があります。このチュートリアルでは、サンプルのソースコードとツールチェーンテンプレートをこの場所にアップロードします。

> **Note**
>
> AWS アカウントには、 で使用される AWS サービスなど、このチュートリアルに関連するコストが請求される場合があります AWS CodeStar。詳細については、「AWS CodeStar 料金」を参照してください。

トピック

ステップ 1: サンプルソースコードのダウンロードと確認

このチュートリアルでは、ダウンロード可能な zip ファイルがあります。Lambda コンピューティングプラットフォームの Node.js サンプルアプリケーションのサンプルソースコードが含まれます。ソースコードをリポジトリに配置したら、フォルダとファイルは次のように表示されます：

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

以下のプロジェクト要素はサンプルソースコードで表されます。

- `tests/`: このプロジェクトの CodeBuild プロジェクト用にユニットテストの設定。このフォルダには、サンプルコードが含まれていますが、プロジェクトの作成には必要ありません。
- `app.js`: プロジェクトのアプリケーションソースコード。

- `buildspec.yml`: CodeBuild リソース構築ステージの構築手順。このファイルは、CodeBuild リソースを含むツールチェーンテンプレートで必要です。
- `package.json`: アプリケーションソースコードの依存関係情報。
- `README.md`: AWS CodeStar のすべてのプロジェクトに含まれるプロジェクトの readme ファイル。このファイルはサンプルコードに含まれていますが、プロジェクトの作成には必要ありません。
- `template.yml`: すべての AWS CodeStar プロジェクトに含まれるインフラストラクチャテンプレートファイルまたは SAM テンプレートファイル。これは、このチュートリアルで後にアップロードするツールチェーン template.yml とは異なります。このファイルはサンプルコードに含まれていますが、プロジェクトの作成には必要ありません。

ステップ 2: サンプルツールチェーンテンプレートのダウンロード

このチュートリアルで提供されるサンプルツールチェーンテンプレートは、リポジトリ (CodeCommit)、パイプライン (CodePipeline)、ビルドコンテナ (CodeBuild) を作成し、CloudFormation を使用してソースコードを Lambda プラットフォームにデプロイします。これらのリソースに加えて、IAM ロール (ランタイム環境のアクセス許可の絞り込みに使用) や、Amazon S3 バケット (CodePipeline によりデプロイメントアーティファクトの保存に使用)、CloudWatch Events ルール (コードをリポジトリにプッシュする際にパイプラインのデプロイのトリガーに使用) もあります。AWS IAM ベストプラクティスに合わせるには、この例で定義されているツールチェーンロールのポリシーを絞り込みます。

サンプル AWS CloudFormation テンプレートを YAML 形式でダウンロードして解凍します。

チュートリアルの後半で create-project コマンドを実行すると、このテンプレートによって、次のカスタマイズされたツールチェーンリソースが CloudFormationで作成されます。このチュートリアルで作成されるリソースの詳細については、『AWS CloudFormation ユーザーガイド』の次のトピックを参照してください。

- AWS::CodeCommit::Repository CloudFormation リソースは CodeCommit リポジトリを作成します。
- AWS::CodeBuild::Project CloudFormation リソースは CodeBuild ビルドプロジェクトを作成します。
- AWS::CodeDeploy::Application CloudFormation リソースは CodeDeploy アプリケーションを作成します。

- AWS::CodePipeline::Pipeline CloudFormation リソースは CodePipeline パイプラインを作成します。
- AWS::S3::Bucket CloudFormation リソースは、パイプラインのアーティファクトバケットを作成します。
- AWS::S3::BucketPolicy CloudFormation リソースは、パイプラインのアーティファクトバケットのアーティファクトバケットポリシーを作成します。
- AWS::IAM::Role CloudFormation リソースは、CodeBuild ビルドプロジェクトを管理するアクセス AWS CodeStar 許可を付与する CodeBuild IAM ワーカーロールを作成します。
- AWS::IAM::Role CloudFormation リソースは、パイプラインを作成する AWS CodeStar アクセス許可を付与する CodePipeline IAM ワーカーロールを作成します。
- AWS::IAM::Role CloudFormation リソースは、リソーススタックを作成する AWS CodeStar アクセス許可を付与する IAM CloudFormation ワーカーロールを作成します。
- AWS::IAM::Role CloudFormation リソースは、リソーススタックを作成する AWS CodeStar アクセス許可を付与する IAM CloudFormation ワーカーロールを作成します。
- AWS::IAM::Role CloudFormation リソースは、リソーススタックを作成する AWS CodeStar アクセス許可を付与する IAM CloudFormation ワーカーロールを作成します。
- AWS::Events::Rule CloudFormation リソースは、プッシュイベントについてリポジトリをモニタリングする CloudWatch Events ルールを作成します。
- AWS::IAM::Role CloudFormation リソースは CloudWatch Events IAM ロールを作成します。

ステップ 3: でツールチェーンテンプレートをテストする CloudFormation

ツールチェーンテンプレートをアップロードする前に、 CloudFormation のツールチェーンテンプレートをテストし、エラーがある場合にはトラブルシューティングすることができます。

1. 更新されたテンプレートをローカルコンピュータに保存し、 CloudFormation コンソールを開きます。[Create Stack] (スタックの作成) を選択します。新しいリソースがリストに表示されています。
2. スタックの作成エラーがないかどうかスタックを確認します。
3. テストが完了したら、スタックを削除します。

> **Note**
>
> スタックと、 で作成されたすべてのリソースを削除してください CloudFormation。削除しない場合は、プロジェクトを作成すると、リソース名が既に使用されているというエラーが表示される場合があります。

ステップ 4: ソースコードとツールチェーンテンプレートのアップロード

AWS CodeStar プロジェクトを作成するには、まずソースコードを .zip ファイルにパッケージ化し、Amazon S3 に配置する必要があります。 はこれらの内容でリポジトリを AWS CodeStar 初期化します。 AWS CLIにプロジェクトを作成するコマンドを実行する際、入力ファイルでこの場所を指定します。

さらに、`toolchain.yml` ファイルをアップロードして、Amazon S3 に置きます。コマンドを実行して でプロジェクトを作成するときに、入力ファイルでこの場所を指定します。 AWS CLI

ソースコードとツールチェーンテンプレートをアップロードするには

1. 以下のサンプルファイル構造は、圧縮およびアップロードされるソースファイルとツールチェーンテンプレートを示します。サンプルコードには、`template.yml` ファイルを含みます。このファイルは、`toolchain.yml` ファイルとは異なる点にご注意ください。

   ```
   ls
   src toolchain.yml

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

2. ソースコードファイルの .zip ファイルを作成します。

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

3. cp コマンドを使用して、パラメータとしてファイルを含めます。

   以下のコマンドにより、.zip ファイルおよび `toolchain.yml` が Amazon S3 にアップロードされます。

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

Amazon S3 バケットを設定してソースコードを共有するには

- ソースコードとツールチェーンを Amazon S3 に保存するため、Amazon S3 バケットポリシーとオブジェクト ACLs を使用して、他の IAM ユーザーまたは AWS アカウントがサンプルからプロジェクトを作成できるようにします。カスタムプロジェクトを作成するすべてのユーザーが、使用するツールチェーンとソースにアクセスできる AWS CodeStar ようにします。

  すべてのユーザーがサンプルを使用できるようにするためには、以下のコマンドを実行します:

```
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
```

ステップ 5: でプロジェクトを作成する AWS CodeStar

プロジェクトを作成するには、以下の手順に従います。

> **Important**
>
> で優先 AWS リージョンを設定してください AWS CLI。プロジェクトは、 で設定された AWS リージョンに作成されます AWS CLI。

1. create-project コマンドを実行し、`--generate-cli-skeleton` パラメータを含めます。

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

   JSON 形式のデータが出力に表示されます。 AWS CLI がインストールされているローカルコンピュータまたはインスタンス上の場所にある ファイル (など*input.json*) にデータをコピーします。コピーされたデータを次のように変更して、結果を保存します。この入力ファイルは、`MyProject` という名前のプロジェクトに、`myBucket` という名前のバケットで設定されています。

- roleArn パラメータを指定していることを確認します。カスタムテンプレートの場合は、このチュートリアルのサンプルテンプレートのように、ロールを指定する必要があります。このロールは、「ステップ 2: サンプルツールチェーンテンプレートのダウンロード」で指定されたすべてのリソースを作成するためのアクセス許可を持っている必要があります。
- stackParameters に ProjectId パラメータを指定していることを確認します。このチュートリアルのサンプルテンプレートでは、このパラメータを使用する必要があります。

```
{
    "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. 保存したばかりのファイルがあるディレクトリに移動し、create-project コマンドをもう一度実行します。--cli-input-json パラメータを指定します。

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

3. 成功すると、次のようなデータが出力に表示されます：

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

- この出力には、新しいプロジェクトに関する情報が含まれています：
  - id 値はプロジェクト ID を表します。
  - arn 値は、プロジェクトの ARN を表します。

4. プロジェクトの作成ステータスを確認するには、describe-project コマンドを使用します。--id パラメータを指定します。

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

次のようなデータが出力に表示されます。

```
{
    "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"
    }
}
```

- この出力には、新しいプロジェクトに関する情報が含まれています：
  - id 値は一意のプロジェクト ID を表します。

- `state` 値は、プロジェクトの作成ステータス (例: `CreateInProgress` または `CreateComplete`) を表します。

プロジェクトが作成される間、コマンドライン またはお好みの IDE からプロジェクトリポジトリに [add team members] (チームメンバーの追加)、または [configure access] (アクセスの設定) を行うことができます。

チュートリアル: AWS CodeStarで Alexa スキルプロジェクトを作成する

AWS CodeStar は、アプリケーションを迅速に開発、構築、デプロイするために必要なツール AWS を提供する のクラウドベースの開発サービスです AWS。を使用すると AWS CodeStar、継続的デリバリーツールチェーン全体を数分でセットアップできるため、コードのリリースをより迅速に開始できます。 AWS CodeStar の Alexa スキルプロジェクトテンプレートを使用すると、数回クリックするだけで、 AWS アカウントからシンプルな Hello World Alexa スキルを作成できます。テンプレートでは、スキル開発用の継続的インテグレーション (CI) ワークフローの使用を開始できる基本的なデプロイパイプラインも作成されます。

から Alexa スキルを作成する主な利点 AWS CodeStar は、 でスキル開発を開始し AWS 、Amazon 開発者アカウントをプロジェクトに接続して、スキルを開発ステージに直接デプロイできることです AWS。また、プロジェクトのすべてのソースコードに関するリポジトリを備えたデプロイ (CI) パイプラインを用意できます。任意の IDE を使用してこのリポジトリを設定し、使い慣れているツールを使用してスキルを作成できます。

前提条件

- https://developer.amazon.com にアクセスして Amazon 開発者アカウントを作成します。 サインアップは無料です。このアカウントが Alexa スキルを所有します。
- AWS アカウントがない場合は、次の手順を使用してアカウントを作成します。

  にサインアップするには AWS

  1. https://aws.amazon.com/「https://www.comit」を開き、 AWS 「アカウントの作成」を選択します。

> **Note**
>
> 以前に認証情報 AWS マネジメントコンソール を使用して AWS アカウントのルートユーザー にサインインしたことがある場合は、別のアカウントにサインインを選択します。IAM 認証情報を使用してすでにコンソールにサインインしている場合は、[AWS アカウントのルートユーザー の認証情報を使ってサインイン] を選択します。[新しい AWS アカウントの作成] を選択します。

2. オンラインの手順に従います。

> **Important**
>
> Alexa スキルプロジェクトの作成後、編集はすべてプロジェクトリポジトリ内でのみ行います。このスキルを、ASK CLI や ASK 開発者コンソールなど他の Alexa Skills Kit ツールを使用して直接編集しないことをお勧めします。これらのツールは、プロジェクトのリポジトリと統合されていません。これらを使用すると、スキルおよびリポジトリコードが同期されません。

ステップ 1: プロジェクトを作成して Amazon 開発者アカウントに接続する

このチュートリアルでは、 AWS Lambdaで実行されている Node.js を使用してスキルを作成します。他の言語でもほとんどの手順は同じです。ただし、スキル名は異なります。選択したプロジェクトテンプレート固有の詳細については、プロジェクトリポジトリ内の README.md ファイルを参照してください。

1. にサインインし AWS マネジメントコンソール、 AWS CodeStar コンソールを https://console.aws.amazon.com/codestar/://www.com で開きます。
2. プロジェクトとそのリソースを作成する AWS リージョンを選択します。Alexa スキルランタイムは、次の AWS リージョンで使用できます。
   - アジアパシフィック (東京)
   - 欧州 (アイルランド)
   - 米国東部 (バージニア北部)
   - 米国西部 (オレゴン)
3. [Create project] (プロジェクトの作成) を選択します。

4. [Choose a project template] (プロジェクトのテンプレートを選択する) ページで、以下を選択します：

   a. [Application type] (アプリケーションの種類) には、[Alexa Skill] (Alexa スキル) を選択します。

   b. [Programming language] (プログラミング言語) には、[Node.js] を選択します。

5. 選択した内容が含まれているボックスを選択します。

6. [Project name] (プロジェクト名) に、プロジェクトの名前 (例: **`My Alexa Skill`**) を入力します。別の名前を使用する場合は、このチュートリアル全体で使用してください。 は、プロジェクト ID のこのプロジェクトの関連識別子 AWS CodeStar を選択します (例: my-alexa-skill)。別のプロジェクト ID が表示された場合は、このチュートリアル全体でそれを使用してください。

7. このチュートリアルではリポジトリに [AWS CodeCommit] を選択し、[リポジトリ名] の値は変更しないでください。

8. [Connect Amazon developer account] (Amazon デベロッパーアカウントを接続) を選択して、スキルをホストする Amazon 開発者アカウントにリンクします。Amazon 開発者アカウントをお持ちでない場合は、まず Amazon Developers からアカウントを作成し、登録を完了してください。

9. Amazon 開発者認証情報を使用してサインインします。[許可] を選択し、[確認] を選択して接続を完了します。

10. Amazon 開発者アカウントに関連付けられた複数のベンダー ID がある場合は、このプロジェクト用に使用するものを選択します。管理者または開発者ロールが割り当てられたアカウントを使用してください。

11. [Next (次へ)] を選択します。

12. (オプション) この AWS リージョン AWS CodeStar で を初めて使用する場合は、IAM ユーザー AWS CodeStar に使用する表示名と E メールアドレスを入力します。[Next (次へ)] を選択します。

13. がプロジェクト AWS CodeStar を作成するまで待ちます。この処理には数分かかることがあります。[Project provisioned] (プロジェクトプロビジョン) バナーが表示されるまで次に進まないでください。

ステップ 2: Alexa Simulator でスキルをテストする

最初のステップでは、 がスキル AWS CodeStar を作成し、Alexa スキル開発ステージにデプロイしました。次は、Alexa Simulator でスキルをテストします。

1. AWS CodeStar コンソールのプロジェクトで、アプリケーションの表示を選択します。Alexa Simulator で新しいタブが開きます。

2. ステップ 1 でプロジェクトに接続したアカウントの Amazon 開発者認証情報を使用してサインインします。
3. [Test] (テスト) の下で [Development] (開発) を選択してテストを有効にします。
4. `ask hello node hello` と入力してください。スキルのデフォルトの呼び出し名は `hello node` です。
5. スキルは `Hello World!` と応答するはずです。

Alexa Simulator でスキルが有効になると、Amazon 開発者アカウントに登録された Alexa 搭載デバイスで呼び出すこともできます。デバイスでスキルをテストするには、「アレクサ、hello node にあいさつするように頼んで」と言います。

Alexa Simulator の詳細については、「開発者コンソールでスキルをテストする」を参照してください。

ステップ 3: プロジェクトリソースを調べる

プロジェクトの作成の一環として、 はユーザーに代わって AWS リソース AWS CodeStar も作成しました。これらのリソースには、CodeCommit を使用したプロジェクトリポジトリ、CodePipeline を使用したデプロイパイプライン、 AWS Lambda 関数が含まれます。これらのリソースにはナビゲーションバーからアクセスできます。例えば、[Repository] (リポジトリ) を選択すると、CodeCommit リポジトリの詳細を表示します。パイプラインのデプロイのステータスは、[Pipeline] (パイプライン) ページに表示されます。ナビゲーションバーで概要を選択すると、プロジェクトの一部として作成された AWS リソースの完全なリストを表示できます。このリストには、各リソースへのリンクが含まれています。

ステップ 4: スキルの応答を変更する

このステップでは、スキルの応答を少し変更して、イテレーションサイクルを理解します。

1. ナビゲーションバーで [Repository] (リポジトリ) を選択します。[Repository name] (リポジトリ名) の下にあるリンクを選択すると、プロジェクトのリポジトリが新しいタブまたはウィンドウで開きます。このリポジトリには、ビルド仕様 (buildspec.yml)、 CloudFormation アプリケーションスタック (template.yml)、readme ファイル、およびスキルパッケージ形式 (プロジェクト構造) のスキルのソースコードが含まれています。
2. [file lambda] > [custom] > [index.js] (Node.js の場合) の順に移動します。このファイルには、リクエスト処理コードが含まれています。これは ASK SDK を使用します。

3. [Edit] (編集) を選択します。
4. 24 行目の文字列 `Hello World!` を、文字列 `Hello. How are you?` に置き換えます。
5. ファイルの末尾までスクロールします。作成者名と、E メールアドレス、およびオプションでコミットメッセージを入力します。
6. [Commit changes] (変更のコミット) を選択してリポジトリに対する変更をコミットします。
7. でプロジェクトに戻り AWS CodeStar 、パイプラインページを確認します。パイプラインがデプロイ中であることが表示されます。
8. パイプラインでデプロイが完了したら、もう一度 Alexa Simulator でスキルをテストします。今度はスキルは `Hello. How are you?` と応答するはずです。

ステップ 5: ローカルワークステーションを設定してプロジェクトリポジトリに接続する

以前は CodeCommit コンソールから直接ソース コードに小さな変更を加えました。このステップでは、ローカルワークステーションを使用してプロジェクトリポジトリを設定し、コマンドラインやお好みの IDE からコードを編集および管理できるようにします。以下の手順は、コマンドラインツールをセットアップする方法について説明します。

1. 必要に応じて AWS CodeStar、 のプロジェクトダッシュボードに移動します。
2. ナビゲーションバーで [IDE]を選択します。
3. [Access your project code] (プロジェクトコードにアクセスする) から[Command line interface] (コマンドラインインターフェイス) の下の[View instructions] (手順の表示) を選択します。
4. 手順に従って、次のタスクを完了します：
   a. Git Downloads などのウェブサイトからローカルワークステーションに Git をインストールします。
   b. CLI AWS をインストールします。詳細については、AWS 「 コマンドラインインターフェイスのインストール」を参照してください。
   c. IAM ユーザーアクセスキーとシークレットキーを使用して AWS CLI を設定します。詳細については、「 CLI AWS の設定」を参照してください。
   d. ローカルワークステーションにプロジェクトの CodeCommit リポジトリのクローンを作成します。詳細については、[Connect to a CodeCommit Repository] (CodeCommit リポジトリに接続する) を参照してください。

次のステップ

このチュートリアルでは、基本的なスキルの開始方法を説明しました。スキル開発の取り組みを継続するには、以下のリソースを参照してください。

- スキルの基礎の理解のために、Alexa 開発者 YouTube チャンネルの「Alexa スキルのしくみ」や他のビデオをご覧ください。
- スキルのさまざまなコンポーネントの理解には、[skill package format] (スキルパッケージの形式)、[skill manifest schemas] (スキルマニフェストのスキーマ)、[interaction model schemas] (対話モデルのスキーマ) のドキュメントをお読みください。
- アイデアをスキルとするために、[Alexa Skills Kit]および[ASK SDK]のドキュメントをお読みください。

チュートリアル:GitHub ソースリポジトリを使用してプロジェクトを作成する

を使用すると AWS CodeStar、プルリクエストを作成、レビュー、およびプロジェクトチームとマージするようにリポジトリを設定できます。

このチュートリアルでは、GitHub リポジトリにサンプルウェブアプリケーションのソースコードを格納したプロジェクト、変更をデプロイするパイプライン、アプリケーションがクラウドでホストされている EC2 インスタンスを作成します。プロジェクトを作成した後、このチュートリアルでは、ウェブアプリケーションのホームページに変更を加える GitHub プルリクエストを作成してマージする方法を説明します。

トピック

- ステップ 1: プロジェクトと GitHub リポジトリの作成
- ステップ 2: ソースコードの表示
- ステップ 3: GitHub プルリクエストの作成

ステップ 1: プロジェクトと GitHub リポジトリの作成

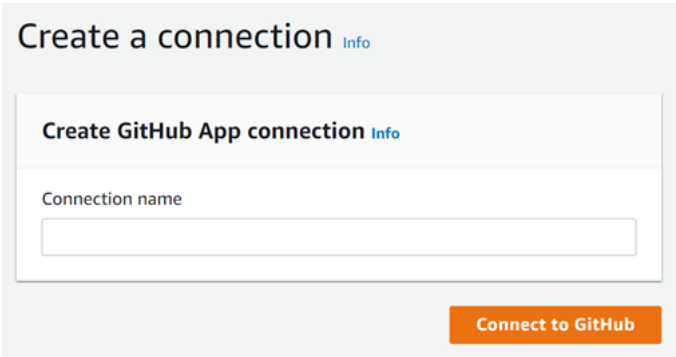
このステップでは、コンソールを使用してプロジェクトを作成し、新しい GitHub リポジトリへの接続を作成します。GitHub リポジトリにアクセスするには、 AWS CodeStar を使用して GitHub で認可を管理する接続リソースを作成します。プロジェクトが作成されると、その追加のリソースがプロビジョンされます。

1. にサインインし AWS マネジメントコンソール、 AWS CodeStar コンソールを https://console.aws.amazon.com/codestar/:///www.com で開きます。
2. プロジェクトとそのリソースを作成する AWS リージョンを選択します。
3. [AWS CodeStar] ページで、[プロジェクトの作成] を選択します。
4. [Choose a project template] (プロジェクトテンプレートを選択する) ページで [Web application] (ウェブアプリケーション)、[Node.js]、および[Amazon EC2] チェックボックスを選択します。次に、オプションのセットで使用可能なテンプレートから選択します。

   詳細については、「AWS CodeStar プロジェクトテンプレート」を参照してください。
5. [Next] (次へ) を選択します。
6. [Project name] (プロジェクト名) に、プロジェクトの名前 (例: **MyTeamProject**) を入力します。別の名前を選択した場合は、このチュートリアル全体でその名前を使用してください。
7. [Project repository] (プロジェクトリポジトリ) で、[GitHub] を選択してください。
8. [GitHub] を選択した場合、接続リソースを選択または作成する必要があります。既存の接続がある場合は、検索フィールドで選択します。それ以外の場合は、ここで新しい接続を作成します。[Connect to GitHub] (GitHub に接続) を選択します。

   [Create a connection] (接続の作成) ページが表示されます。

   > **Note**
   >
   > 接続を作成するには、GitHub アカウントが必要です。組織の接続を作成する場合は、組織の所有者である必要があります。



   a. [Create GitHub App connection] (GitHub App 接続の作成) で、[Connection name] (接続名) に接続名を入力します。[Connect to GitHub] (GitHub に接続) を選択します。

[Connect to GitHub] (GitHub に接続) ページが表示され、[GitHub Apps] フィールドが表示されます。

b. [GitHub Apps] で、アプリケーションのインストールを選択するか、[Install a new app] (新しいアプリケーションをインストールする) を選択してアプリケーションを作成します。

> **Note**
>
> 特定のプロバイダーへのすべての接続に対してアプリを 1 つインストールします。AWS Connector for GitHub アプリをすでにインストールしている場合は、それを選択してこのステップをスキップします。

c. 「Install AWS Connector for GitHub」ページで、アプリをインストールするアカウントを選択します。

> **Note**
>
> アプリケーションをインストール済みである場合は、[Configure] (設定) を選択してアプリのインストールの変更ページに進むか、戻るボタンでコンソールに戻ることができます。

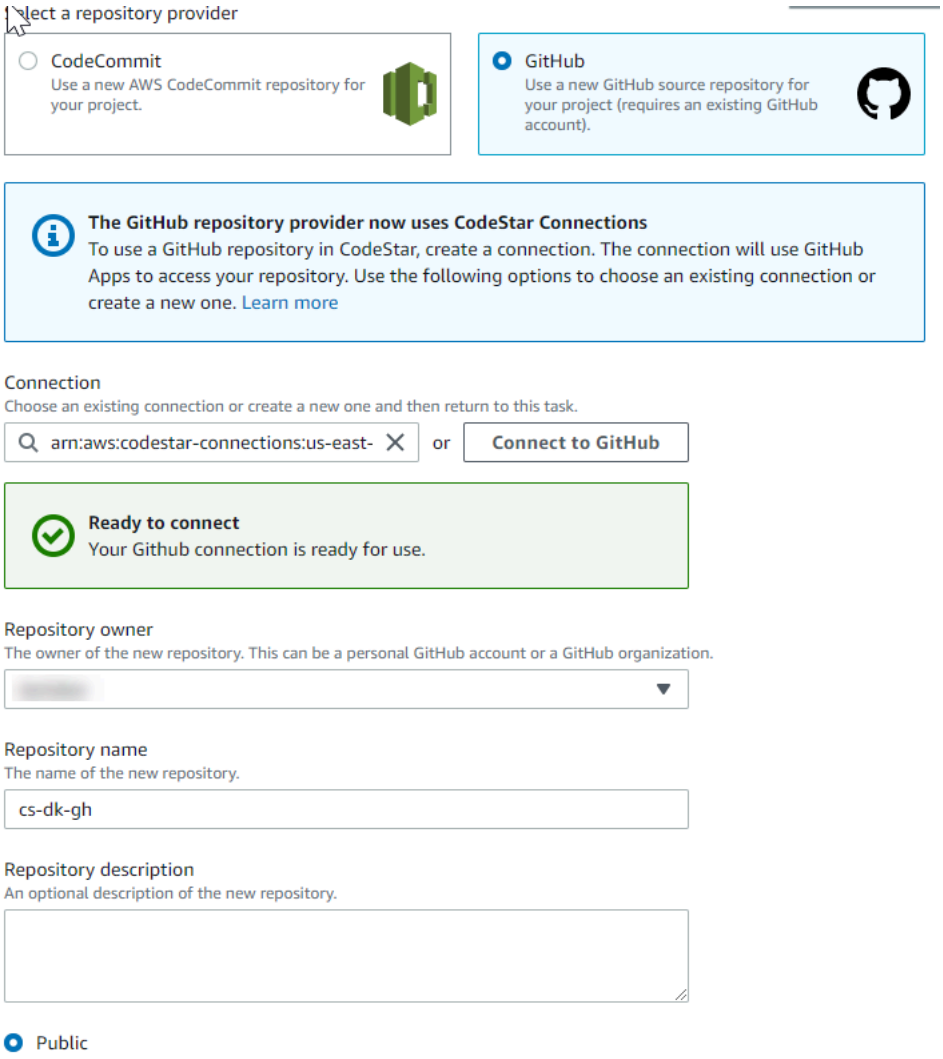
d. [Confirm password to continue] (パスワードを確認して続行) ページが表示される場合、GitHub パスワードを入力し、[Sign in] (サインイン) を選択します。

e. GitHub 用 AWS コネクタのインストールページで、デフォルトのままにして、インストールを選択します。

f. [Connect to GitHub] (GitHub へ接続) ページで、新規インストールのインストール ID が [GitHub Apps] に表示されます。

接続が正常に作成された後、CodeStar の [create project] (プロジェクトを作成) ページで、[Ready to connect] (接続準備完了) メッセージが表示されます。

> **Note**
>
> [Developer Tools] (デベロッパーツール) コンソールの [Settings] (設定) で接続を表示できます。詳細については、[Getting started with connections] (接続入門ガイド) を参照してください。



g. [Repository owner] (リポジトリ所有者) で、GitHub 組織または個人用 GitHub アカウントを選択します。

h. [Repository name] (リポジトリ名) で、デフォルトの GitHub リポジトリ名を受け入れるか、別の名前を入力します。

i. [Public] (公開) または[Private] (プライベート) を選択します。

> **Note**
>
> 開発環境 AWS Cloud9 として を使用する場合は、パブリックリポジトリを選択する必要があります。

j. (オプション) [Repository description] (リポジトリの説明) に、GitHub リポジトリの説明を入力します。

9. プロジェクトが Amazon EC2 インスタンスにデプロイされ、変更する場合、[Amazon EC2 Configuration](Amazon EC2 の設定)で Amazon EC2 インスタンスを設定します。例えば、プロジェクトの使用可能なインスタンスタイプから選択できます。

   [key pair] (キーペア) で、ステップ 4: AWS CodeStar プロジェクトの Amazon EC2 キーペアの作成 で作成した Amazon EC2 キーペアを選択します。[I acknowledge that I have access to the private key file] (私はプライベートキーファイルへのアクセス権があることを認めます) を選択します。

10. [Next] (次へ) を選択します。
11. リソースと設定の詳細を確認します。
12. [Next] (次へ) または [Create project] (プロジェクトの作成) を選択します。(表示される選択はプロジェクトテンプレートによって異なります。)

    プロジェクトの作成中は、数分間待ってください。

13. プロジェクトが作成された後、[アプリケーションの表示] を選択して、ウェブアプリケーションを表示します。

ステップ 2: ソースコードの表示

このステップでは、ソースコードとソースリポジトリに使用できるツールを表示します。

1. プロジェクトのナビゲーションバーで、[Repository] (リポジトリ) を選択します。

   GitHub でコミットのリストを表示するには、[View commits] (コミットの表示) を選択します。これにより GitHub でコミット履歴が開きます。

   課題を表示するには、プロジェクトの [Issues] (課題) タブを選択します。GitHub で新しい課題を作成するには、[Create GitHub issue] (GitHub の課題を作成する) を選択します。これにより、GitHub でリポジトリの課題フォームが開きます。

2. [Repository] (リポジトリ) タブで、[Repository name] (リポジトリ名) の下にあるリンクを選択すると、プロジェクトのリポジトリが新しいタブまたはウィンドウで開きます。このリポジトリには、プロジェクトのソースコードが含まれています。

ステップ 3: GitHub プルリクエストの作成

このステップでは、ソースコードにわずかな変更を加え、プルリクエストを作成します。

1. GitHub で、リポジトリに新しい機能ブランチを作成します。[main branch] (メインブランチ) ドロップダウンフィールドを選択し、`feature-branch` という名前のフィールドに新しいブランチを入力します。[Create new branch] (新規ブランチを作成) を選択します。ブランチが作成され、チェックアウトされます。
2. GitHub で、`feature-branch`ブランチに変更を加えます。公開フォルダを開き、`index.html` ファイルを開きます。
3. AWS CodeStar コンソールのプルリクエストで、GitHub でプルリクエストを作成するには、プルリクエストの作成を選択します。これにより、GitHub でリポジトリのプルリクエストフォームが開きます。GitHub で、鉛筆アイコンを選択してファイルを編集します。

   `Congratulations!` の後、文字列 `Well done, <name>!` を追加してユーザーの名前で `<name>` を置き換えます。[Commit changes] (変更のコミット) を選択します。変更は機能ブランチにコミットされます。
4. AWS CodeStar コンソールで、プロジェクトを選択します。[Repository] (リポジトリ) タブを選択します。[Pull requests] (プルリクエスト) で、[Create pull request] (プルリクエストの作成) を選択します。

   GitHub でフォームが開きます。メインブランチはベースブランチに残します。[Compare to] (比較する) で、機能ブランチを選択します。差分を表示します。
5. GitHub で、[Create pull request] (プルリクエストの作成) を選択します。[Update index.html] (index.htmlの更新) という名前のプルリクエストが作成されます。
6. AWS CodeStar コンソールで、新しいプルリクエストを表示します。[Merge changes] (マージ変更) を選択して、変更をリポジトリにコミットし、プルリクエストをリポジトリのメインブランチとマージします。
7. でプロジェクトに戻り AWS CodeStar 、パイプラインページを確認します。パイプラインがデプロイ中であることが表示されます。
8. プロジェクトが作成された後、[アプリケーションの表示] を選択して、ウェブアプリケーションを表示します。

AWS CodeStar プロジェクトテンプレート

AWS CodeStar プロジェクトテンプレートを使用すると、サンプルアプリケーションから開始し、開発プロジェクトをサポートするために作成された AWS リソースを使用してデプロイできます。AWS CodeStar プロジェクトテンプレートを選択すると、アプリケーションタイプ、プログラミング言語、コンピューティングプラットフォームがプロビジョニングされます。ウェブアプリケーション、ウェブサービス、Alexa スキル、および静的ウェブページを使用してプロジェクトを作成したら、サンプルアプリケーションを独自のものに置き換えることができます。

がプロジェクト AWS CodeStar を作成したら、application. AWS CodeStar works の配信をサポートする AWS リソースを変更 AWS CloudFormation して、コードを使用してクラウドでサポートサービスとサーバー/サーバーレスプラットフォームを作成できます。 AWS CloudFormation を使用すると、インフラストラクチャ全体をテキストファイルでモデル化できます。

トピック

AWS CodeStar プロジェクトファイルとリソース

AWS CodeStar プロジェクトは、ソースコードとコードをデプロイするために作成されたリソースの組み合わせです。コードのビルド、リリース、デプロイに役立つリソースのコレクションは、[Toolchain resources] (ツールチェーンリソース) と呼ばれます。プロジェクト作成時、CloudFormation テンプレートを使用して、継続的な統合/継続的デプロイメント (CI/CD) パイプラインのツールチェーンリソースをプロビジョンします。

AWS CodeStar を使用して、 AWS リソース作成の経験レベルに応じて、次の 2 つの方法でプロジェクトを作成できます。

- コンソールを使用してプロジェクトを作成すると、 はリポジトリを含むツールチェーンリソース AWS CodeStar を作成し、リポジトリにサンプルアプリケーションコードとプロジェクトファイルを入力します。コンソールを使用して、事前設定済みのプロジェクトオプションのセットに基づき、サンプルプロジェクトをすばやくセットアップできます。
- CLI を使用してプロジェクトを作成する場合は、ツールチェーンリソースとアプリケーションのソースコードを作成する CloudFormation テンプレートを指定します。CLI を使用して、 AWS

CodeStar がテンプレートからプロジェクトを作成し、リポジトリにサンプルコードを入力します。

AWS CodeStar プロジェクトは、単一の管理ポイントを提供します。コンソールで [Create project] (プロジェクトの作成) ウィザードを使用して、サンプルプロジェクトをセットアップします。チームのアクセス許可とリソースを管理するコラボレーションプラットフォームとして使用できます。詳細については、「とは AWS CodeStar」を参照してください。コンソールを使用してプロジェクトを作成すると、ソースコードがサンプルコードとして提供され、CI/CD ツールチェーンリソースが作成されます。

コンソールでプロジェクトを作成すると、 は次のリソースを AWS CodeStar プロビジョニングします。

- GitHub または CodeCommit のソースコードリポジトリ。
- ファイルとディレクトリの詳細を提供する `README.md` ファイル (プロジェクトリポジトリ内)。
- アプリケーションのランタイムスタックの定義を保存する `template.yml` ファイル (プロジェクトリポジトリ内)。このファイルを使用して、通知、データベースのサポート、モニタリング、トレースに使用されるリソースなど、ツールチェーンリソースではないプロジェクト AWS リソースを追加または変更します。
- AWS Amazon S3 アーティファクトバケット、Amazon CloudWatch Events、関連するサービスロールなど、パイプラインに関連して作成された サービスとリソース。
- 完全なソースコードとパブリック HTTP エンドポイントを含む実動するサンプルアプリケーション。
- AWS CodeStar プロジェクトテンプレートタイプに基づく AWS コンピューティングリソース :
  - Lambda 関数。
  - Amazon EC2 インスタンス。
  - AWS Elastic Beanstalk 環境。
- 2018 年 12 月 6 日 (PDT) スタート:
  - アクセス許可の境界 (プロジェクトリソースへのアクセスを管理するための特殊な IAM ポリシー)。アクセス許可の境界は、デフォルトでサンプルプロジェクトのロールに添付されています。詳細については、「ワーカーロールの IAM アクセス許可の境界」を参照してください。
  - IAM CloudFormation ロールを含む、 CloudFormation サポートされているすべてのリソースに対するアクセス許可 CloudFormation を含む、 を使用してプロジェクトリソースを作成するための IAM ロール。

- ツールチェーンの IAM ロール。
- アプリケーションスタックで定義された Lambda の実行ロール (変更可能)。

- 2018 年 12 月 6 日 (PDT) 以前:
  - 限られたリソースのセットをサポートするプロジェクト CloudFormation リソースを作成するための CloudFormation IAM ロール。
  - CodePipeline リソースを作成するための IAM ロール。
  - CodeBuild リソースを作成するための IAM ロール。
  - プロジェクトタイプで該当する場合、CodeDeploy リソースを作成するための IAM ロール。
  - プロジェクトタイプで該当する場合、Amazon EC2 ウェブアプリケーションを作成するための IAM ロール。
  - CloudWatch Events リソースを作成するための IAM ロール。
  - 動的に変更され、リソースの一部を含めるための Lambda の実行ロール。

このプロジェクトには、ステータスを示す詳細ページがあり、チーム管理へのリンク、IDE またはリポジトリの設定手順へのリンク、リポジトリ内のソースコード変更のコミット履歴が含まれています。また、Jira などの外部の課題追跡ツールに接続するためのツールを選択することもできます。

はじめに: プロジェクトテンプレートを選択する

コンソールで AWS CodeStar プロジェクトを選択すると、サンプルコードとリソースを含む事前設定されたオプションのセットから選択して、すぐに開始できます。これらのオプションは、[Project templates] (プロジェクトテンプレート) と呼ばれます。各 AWS CodeStar プロジェクトテンプレートは、プログラミング言語、アプリケーションタイプ、コンピューティングプラットフォームで構成されます。プロジェクトテンプレートは、選択した組み合わせによって決まります。

テンプレートコンピューティングプラットフォームを選択する

テンプレートごとに、次のコンピューティングプラットフォームタイプのいずれかを設定します。

- AWS Elastic Beanstalk プロジェクトを選択するときは、クラウド内の AWS Elastic Beanstalk Amazon Elastic Compute Cloud インスタンスの環境にデプロイします。
- Amazon EC2 プロジェクトを選択すると、 は Linux EC2 インスタンス AWS CodeStar を作成し、アプリケーションをクラウドでホストします。プロジェクトチームメンバーはインスタンスにアクセスでき、チームは指定したキーペアを使用して Amazon EC2 インスタンスに SSH 接続しま

す。 には、チームメンバーのアクセス許可を使用してキーペア接続を管理するマネージド SSH AWS CodeStar もあります。

- 選択すると AWS Lambda、 は Amazon API Gateway 経由でアクセスするサーバーレス環境 AWS CodeStar を作成し、維持するインスタンスやサーバーはありません。

テンプレートアプリケーションタイプを選択する

テンプレートごとに、次のアプリケーションタイプのいずれかを設定します：

- ウェブサービス

  ウェブサービスは、API を呼び出すなど、バックグラウンドで実行されるタスクに使用されます。がサンプルウェブサービスプロジェクト AWS CodeStar を作成したら、エンドポイント URL を選択して Hello World 出力を表示できますが、このアプリケーションタイプの主な用途はユーザーインターフェイス (UI) ではありません。このカテゴリの AWS CodeStar プロジェクトテンプレートは、Ruby、Java、ASP.NET://www.com、PHP、Node.js などの開発をサポートしています。

- ウェブアプリケーション

  ウェブアプリケーションには、UI が搭載されています。がサンプルウェブアプリケーションプロジェクト AWS CodeStar を作成したら、エンドポイント URL を選択してインタラクティブなウェブアプリケーションを表示できます。このカテゴリの AWS CodeStar プロジェクトテンプレートは、Ruby、Java、ASP.NET://www.com、PHP、Node.js などの開発をサポートしています。

- 静的ウェブページ

  HTML ウェブサイトのプロジェクトが必要な場合はこのテンプレートを選択します。このカテゴリの AWS CodeStar プロジェクトテンプレートは、HTML5 の開発をサポートします。

- Alexa スキル

  このテンプレートを選択するのは、Alexa スキルのプロジェクトで AWS Lambda 関数を使用する場合のみです。スキルプロジェクトを作成すると、AWS CodeStar によってサービスエンドポイントとして使用できる Amazon リソースネーム (ARN) が返されます。詳細については、「カスタムスキルを AWS Lambda 関数としてホストする」を参照してください。

> **Note**
>
> Alexa スキルの Lambda 関数は、米国東部 (バージニア北部)、米国西部 (オレゴン)、欧州 (アイルランド)、およびアジアパシフィック (東京) の各リージョンでのみサポートされています。

- Config ルール

  アカウント内の AWS リソース間でルールを自動化できる AWS Config ルールのプロジェクトが必要な場合は、このテンプレートを選択します。この関数は、ルールのサービスエンドポイントとして使用できる ARN を返します。

テンプレートのプログラミング言語の選択

プロジェクトテンプレートを選択する際、Ruby、Java、ASP.NET、PHP、Node.js などのプログラミング言語を選択します。

AWS CodeStar プロジェクトに変更を加える方法

プロジェクトを更新するには、以下を更新します：

- アプリケーションのサンプルコードおよびプログラミング言語リソース。
- アプリケーションが保存およびデプロイされるインフラストラクチャを構成するリソース (オペレーティングシステム、サポートアプリケーションとサービス、デプロイパラメータ、クラウドコンピューティングプラットフォーム)。アプリケーションリソースは、`template.yml` ファイルで変更します。これは、アプリケーションのランタイム環境をモデリングする AWS CloudFormation ファイルです。

> **Note**
>
> Alexa Skills AWS CodeStar プロジェクトを使用している場合、 AWS CodeStar ソースリポジトリ (CodeCommit または GitHub) の外部でスキルを変更することはできません。Alexa デベロッパーポータルでスキルを編集すると、その変更がソースリポジトリに表示されない場合があり、2 つのバージョンは同期しません。

アプリケーションソースコードの変更と変更のプッシュ

サンプルソースコード、スクリプト、および他のアプリケーションソースファイルを変更するには、ソースリポジトリのファイルを次のように編集します：

- CodeCommit または GitHub の編集モードを使用する。
- などの IDE でプロジェクトを開きます AWS Cloud9。
- リポジトリのクローンをローカルに作成後、変更をコミットおよびプッシュします。詳細については、ステップ 4: 変更をコミットする を参照してください。

Template.yml ファイルを使用してアプリケーションリソースを変更する

インフラストラクチャリソースを手動で変更する代わりに、 AWS CloudFormation を使用してアプリケーションのランタイムリソースをモデル化してデプロイします。

ランタイムスタックのアプリケーションリソース (例: Lambda 関数) を変更または追加するには、プロジェクトリポジトリの `template.yml` ファイルを編集します。 AWS CloudFormation リソースとして利用可能なリソースを追加することができます。

AWS Lambda 関数のコードまたは設定を変更するには、「」を参照してくださいリソースをプロジェクトに追加する。

プロジェクトのリポジトリの `template.yml` ファイルを変更して、アプリケーション AWS CloudFormation リソースであるリソースのタイプを追加します。`template.yml` ファイルの `Resources`セクションにアプリケーションリソースを追加 AWS CloudFormation し、そのリソース AWS CodeStar を作成する場合。 AWS CloudFormation リソースとその必要なプロパティのリストについては、AWS 「リソースタイプのリファレンス」を参照してください。詳細については、「ステップ 1: IAM で CloudFormation ワーカーロールを編集する」のこの例を参照してください。

AWS CodeStar では、アプリケーションのランタイム環境を設定およびモデリングすることで、ベストプラクティスを実装できます。

アプリケーションリソースを変更するアクセス許可を管理する方法

AWS CloudFormation を使用して Lambda 関数などのランタイムアプリケーションリソースを追加する場合、 AWS CloudFormation ワーカーロールは、既に持っているアクセス許可を使用できま

す。一部のランタイムアプリケーションリソースでは、`template.yml` ファイルを編集する前に、AWS CloudFormation ワーカーロールのアクセス許可を手動で調整する必要があります。

AWS CloudFormation ワーカーロールのアクセス許可を変更する例については、「」を参照してくださいステップ 5: インラインポリシーでリソースのアクセス許可を追加する。

AWS CodeStar ベストプラクティス

AWS CodeStar は、多くの 製品やサービスと統合されています。以下のセクションでは、 AWS CodeStar およびこれらの関連製品およびサービスのベストプラクティスについて説明します。

トピック

AWS CodeStar リソースで使用するセキュリティのベストプラクティス

定期的にパッチを適用し、アプリケーションで使用される依存関係のセキュリティベストプラクティスを確認する必要があります。これらのセキュリティのベストプラクティスを使用して、サンプルコードを更新し、本番環境でプロジェクトを維持します。

- 進行中のセキュリティに関する発表と、フレームワークの更新を追跡します。
- プロジェクトをデプロイする前に、フレームワークで開発されたベストプラクティスに従います。
- フレームワークの依存関係を定期的に確認し、必要に応じて更新します。
- 各 AWS CodeStar テンプレートには、プログラミング言語の設定手順が含まれています。プロジェクトのソースリポジトリの `README.md` ファイルを参照してください。
- プロジェクトリソースを分離するためのベストプラクティスとして、のセキュリティ AWS CodeStar に導入された [multi-account strategy] (マルチアカウント戦略) を使用して AWS リソースへの最小特権アクセスを管理します。

依存関係のバージョンを設定するベストプラクティス

AWS CodeStar プロジェクトのサンプルソースコードは、ソースリポジトリの `package.json` ファイルに記載されている依存関係を使用します。ベストプラクティスとして、常に特定のバージョンを指すように依存関係を設定します。これは、バージョンピンニングとも呼ばれます。予告なしにアプリケーションが中断する可能性があるため、バージョンを `latest` に設定することはお勧めしません。

AWS CodeStar リソースで使用するモニタリングと ログ記録のベストプラクティス

の ログ記録機能を使用して AWS 、ユーザーがアカウントで実行したアクションと使用されたリソースを判断できます。ログファイルは次の情報を表示します：

- アクションが実行された日時。
- アクションのソース IP アドレス。
- 不適切なアクセス権限が理由で失敗したアクション。

AWS CloudTrail は、 AWS アカウントによって、またはアカウントに代わって行われた AWS API コールおよび関連イベントの ログ記録に使用できます。詳細については、「を使用した AWS CodeStar API コールの ログ記録 AWS CloudTrail」を参照してください。

でのプロジェクトの使用 AWS CodeStar

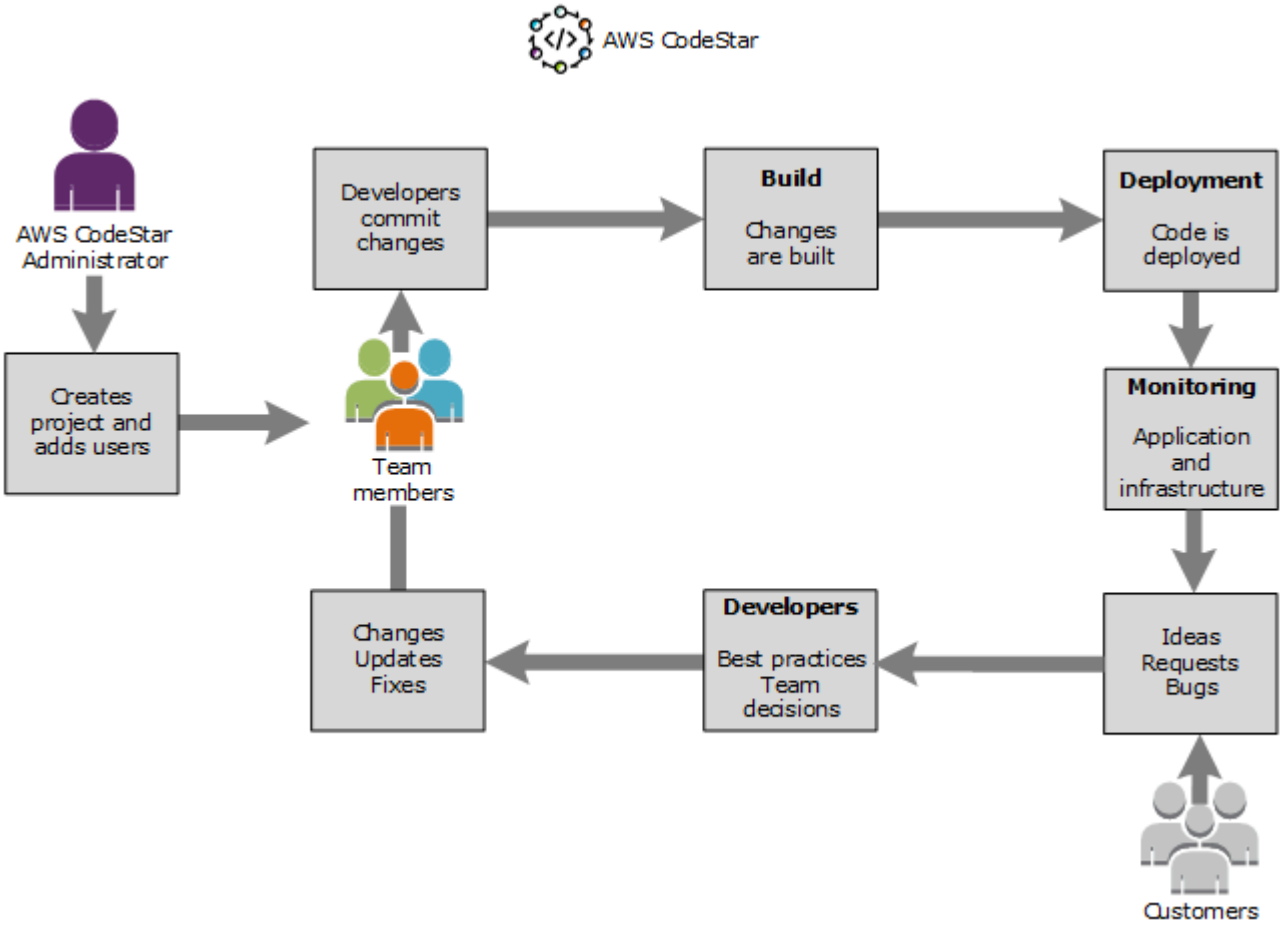
AWS CodeStar プロジェクトテンプレートを使用すると、以下を含む必要なリソースですでに設定されたプロジェクトをすばやく作成できます。

- ソースリポジトリ
- 構築環境
- デプロイとホスティングリソース
- プログラム言語

テンプレートにはサンプルソースコードも含まれているため、すぐにプロジェクトで作業を開始できます。

プロジェクトを作成すると、リソースの追加や削除、プロジェクトダッシュボードのカスタマイズ、進行状況のモニタリングを行うことができます。

次の図は、 AWS CodeStar プロジェクトの基本的なワークフローを示しています。



図の基本のワークフローでは、AWSCodeStarFullAccess ポリシーを適用したデベロッパーがプロジェクトを作成し、チームメンバーを追加します。一緒にコードを書き込み、ビルド、テスト、およびデプロイします。プロジェクトダッシュボードには、アプリケーションアクティビティの表示とビルドのモニタリング、デプロイメントパイプラインを介したコードの流れの表示などをリアルタイムで使用できるツールが提供されます。チームは、チーム wiki タイルを使用して、情報、ベストプラクティス、リンクを共有します。問題追跡ソフトウェアを統合して、進行状況やタスクを追跡するのに役立ちます。お客様からリクエストやフィードバックを受け取ると、チームはこの情報をプロジェクトに追加し、プロジェクト計画および開発に統合します。プロジェクトが成長するにつれて、チームはそのコードベースをサポートするために、より多くのチームメンバーを追加します。

でプロジェクトを作成する AWS CodeStar

AWS CodeStar コンソールを使用してプロジェクトを作成します。プロジェクトテンプレートを使用する場合は、お客様に必要なリソースが設定されます。このテンプレートには、コーディングを開始するために使用するサンプルコードも含まれています。

プロジェクトを作成するには、 AWSCodeStarFullAccessポリシーまたは同等のアクセス許可を持つ IAM ユーザー AWS マネジメントコンソール を使用して にサインインします。詳細については、「AWS CodeStarのセットアップ」を参照してください。

> **Note**
>
> このトピックで手順を完了する前に、AWS CodeStarのセットアップ のステップを完了する必要があります。

トピック

- AWS CodeStar コンソールでプロジェクトを作成する (コンソール)
- (AWS CodeStar AWS CLI) でプロジェクトを作成する

AWS CodeStar コンソールでプロジェクトを作成する (コンソール)

AWS CodeStar コンソールを使用してプロジェクトを作成します。

でプロジェクトを作成するには AWS CodeStar

1. にサインインし AWS マネジメントコンソール、 AWS CodeStar コンソールを https://console.aws.amazon.com/codestar/://www.com で開きます。

   プロジェクトとそのリソースを作成する AWS リージョンにサインインしていることを確認します。たとえば、米国東部 (オハイオ) でプロジェクトを作成するには、その AWS リージョンが選択されていることを確認してください。 AWS CodeStar が利用可能な AWS リージョンの詳細については、 AWS 全般のリファレンスの「リージョンとエンドポイント」を参照してください。
2. [AWS CodeStar] ページで、[プロジェクトの作成] を選択します。
3. プロジェクトテンプレートの選択ページで、プロジェクトテンプレートのリストから AWS CodeStar プロジェクトタイプを選択します。フィルタバーを使用して選択を絞り込むことができます。例えば、Amazon EC2 インスタンスにデプロイされる Node.js で記述されたウェブアプリケーションプロジェクトの場合は、[Web application] (ウェブアプリケーション)、[Node.js] の順に選択し、[Amazon EC2] チェックボックスをオンにします。次に、オプションのセットで使用可能なテンプレートから選択します。

   詳細については、「AWS CodeStar プロジェクトテンプレート」を参照してください。

4. [Next (次へ)] を選択します。
5. [プロジェクト名] で、*My First Project* などのプロジェクト名を入力します。[Project ID] (プロジェクト ID) では、プロジェクトの ID はこのプロジェクト名から派生しますが、15 文字の制限があります。

   例えば、*My First Project* という名前のプロジェクトのデフォルト ID は *my-first-projec* です。このプロジェクト ID は、プロジェクトに関連付けられているすべてのリソースの名前のベースです。 AWS CodeStar は、このプロジェクト ID をコードリポジトリの URL の一部として使用するほか、IAM の関連するセキュリティアクセスロールとポリシーの名前にも使用します。プロジェクトの作成後、プロジェクト ID は変更できません。プロジェクトを作成する前にプロジェクト ID を編集するには、[Project ID] (プロジェクト ID) で、使用する ID を入力します。

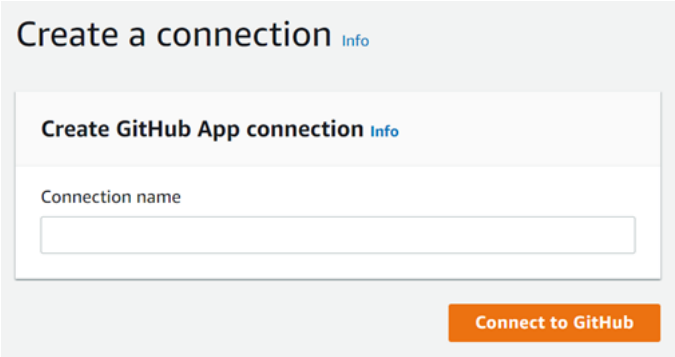
   プロジェクト名とプロジェクト ID の制限の詳細については、の制限 AWS CodeStar を参照してください。

   > **Note**
   >
   > プロジェクト IDsは、 AWS リージョンの AWS アカウントで一意である必要があります。

6. リポジトリプロバイダー、AWS CodeCommit または [GitHub] を選択します。
7. を選択した場合AWS CodeCommitは、リポジトリ名にデフォルトの AWS CodeCommit リポジトリ名を使用するか、別のリポジトリ名を入力します。ステップ 9 に進みます。
8. [GitHub] を選択した場合、接続リソースを選択または作成する必要があります。既存の接続がある場合は、検索フィールドで選択します。それ以外の場合は、ここで新しい接続を作成します。[Connect to GitHub] (GitHub に接続) を選択します。

   [Create a connection] (接続の作成) ページが表示されます。

   > **Note**
   >
   > 接続を作成するには、GitHub アカウントが必要です。組織の接続を作成する場合は、組織の所有者である必要があります。



a. [GitHub App 接続の作成] で、[接続名] テキスト入力フィールドに接続名を入力します。[Connect to GitHub] (GitHub に接続) を選択します。

   [Connect to GitHub] (GitHub に接続) ページが表示され、[GitHub Apps] フィールドが表示されます。

b. [GitHub Apps] で、アプリケーションのインストールを選択するか、[Install a new app] (新しいアプリケーションをインストールする) を選択してアプリケーションを作成します。

> **Note**
>
> 特定のプロバイダーへのすべての接続に対してアプリを 1 つインストールします。AWS Connector for GitHub アプリをすでにインストールしている場合は、それを選択してこのステップをスキップします。

c. 「Install AWS Connector for GitHub」ページで、アプリをインストールするアカウントを選択します。

> **Note**
>
> アプリケーションをインストール済みである場合は、[Configure] (設定) を選択してアプリのインストールの変更ページに進むか、戻るボタンでコンソールに戻ることができます。

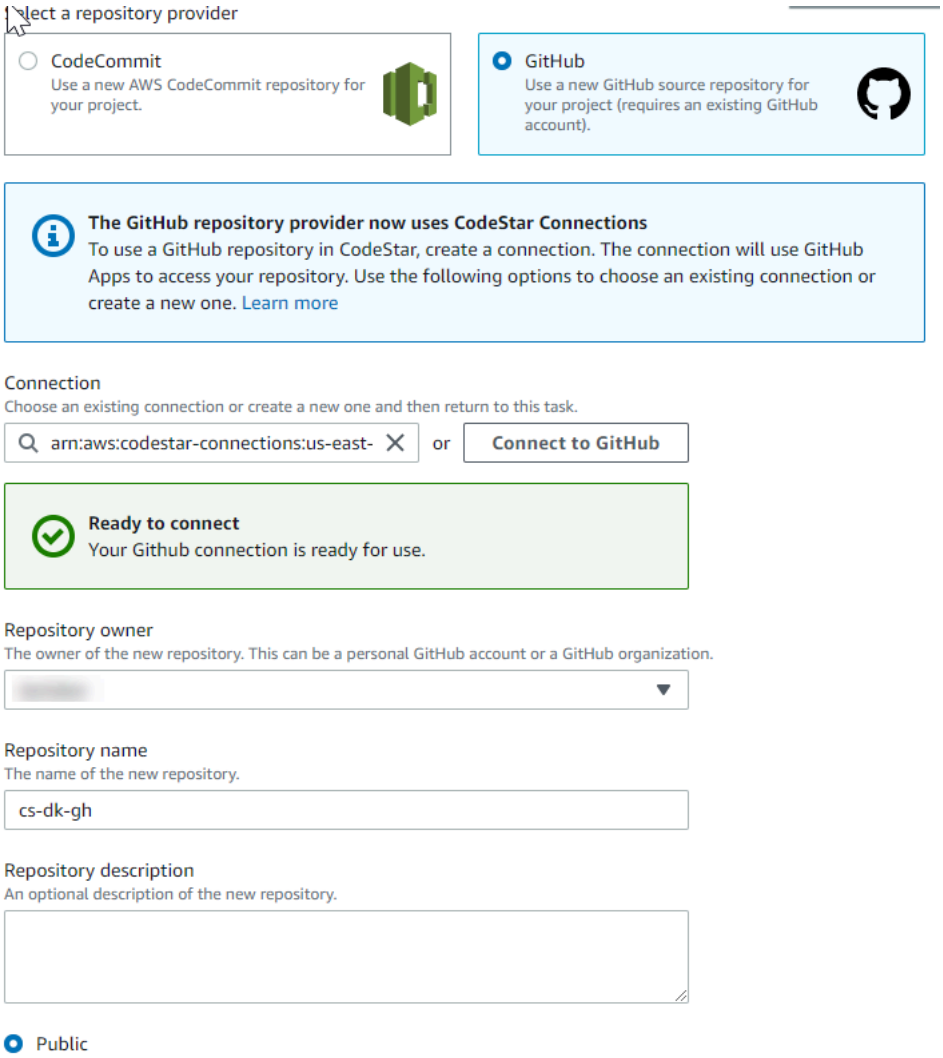
d. [Confirm password to continue] (パスワードを確認して続行) ページが表示される場合、GitHub パスワードを入力し、[Sign in] (サインイン) を選択します。

e. GitHub 用 AWS コネクタのインストールページで、デフォルトのままにして、インストールを選択します。

f. [GitHub へ接続] ページで、新規インストールのインストール ID が [GitHub Apps] テキスト入力フィールドに表示されます。

接続が作成された後、CodeStar の [create project] (プロジェクトを作成) ページで、[Ready to connect] (接続準備完了) メッセージが表示されます。

> **Note**
>
> [Developer Tools] (デベロッパーツール) コンソールの[Settings] (設定) で接続を表示できます。詳細については、[Getting started with connections] (接続入門ガイド) を参照してください。



g. [Repository owner] (リポジトリ所有者) で、GitHub 組織または個人用 GitHub アカウントを選択します。

h. [Repository name] (リポジトリ名) で、デフォルトの GitHub リポジトリ名を受け入れるか、別の名前を入力します。

i. [Public] (公開) または[Private] (プライベート) を選択します。

> **Note**
>
> を開発環境 AWS Cloud9 として使用するには、パブリックを選択する必要があります。

j. (オプション) [Repository description] (リポジトリの説明) に、GitHub リポジトリの説明を入力します。

> **Note**
>
> Alexa スキルプロジェクトテンプレートを選択する場合は、Amazon 開発者アカウントを接続する必要があります。Alexa スキルプロジェクトの操作の詳細については、「チュートリアル: AWS CodeStarで Alexa スキルプロジェクトを作成する」を参照してください。

9. プロジェクトが Amazon EC2 インスタンスにデプロイされ、変更を加える場合は、[Amazon EC2 Configuration] (Amazon EC2 の設定) で Amazon EC2 インスタンスを設定します。例えば、プロジェクトの使用可能なインスタンスタイプから選択できます。

> **Note**
>
> 異なる Amazon EC2 インスタンスタイプは、異なるレベルのコンピューティングパワーを提供し、異なる関連費用が発生する可能性があります。詳細については、[Amazon EC2 Instance Types] (Amazon EC2 インスタンスタイプ) と [Amazon EC2 Pricing] (Amazon EC2 の料金) を参照してください。
> 複数の仮想プライベートクラウド (VPC) または複数のサブネットが Amazon 仮想プライベートクラウド で作成されている場合は、使用する VPC とサブネットを選択することもできます。ただし、ハードウェア専有インスタンスでサポートされていない Amazon EC2 インスタンスタイプを選択した場合は、インスタンスのテナンシーが [Dedicated] (専有) に設定されている VPC を選択することはできません。

詳細については、[What Is Amazon VPC?] (Amazon VPC とは) および [Dedicated Instance Basics] (ハードウェア専有インスタンスの基礎) を参照してください。

[Key pair] (キーペア) で、ステップ 4: AWS CodeStar プロジェクトの Amazon EC2 キーペアの作成 で作成した Amazon EC2 キーペアを選択します。[I acknowledge that I have access to the private key file] (私はプライベートキーファイルへのアクセス権があることを認めます) を選択します。

10. [Next] (次へ) を選択します。
11. リソースと設定の詳細を確認します。
12. [Next] (次へ) または [Create project] (プロジェクトの作成) を選択します。(表示される選択はプロジェクトテンプレートによって異なります。)

    プロジェクト (リポジトリを含む) の作成には数分かかる場合があります。
13. プロジェクトのリポジトリの作成後は、[Repository] (リポジトリ) ページを使用して、リポジトリへのアクセス権を設定します。[Next steps] (次のステップ) のリンクを使用して、IDE を設定、課題追跡を設定、チームメンバーをプロジェクトに追加できます。

プロジェクトが作成される間、コマンドライン またはお好みの IDE からプロジェクトリポジトリに [add team members] (チームメンバーの追加)、または [configure access] (アクセスの設定) を行うことができます。

(AWS CodeStar AWS CLI) でプロジェクトを作成する

AWS CodeStar プロジェクトは、ソースコードとコードをデプロイするために作成されたリソースの組み合わせです。コードのビルド、リリース、デプロイに役立つリソースのコレクションは、ツールチェーンリソースと呼ばれます。プロジェクトの作成時に、 CloudFormation テンプレートはツールチェーンリソースを継続的インテグレーション/継続的デプロイ (CI/CD) パイプラインにプロビジョニングします。

コンソールでプロジェクトを作成すると、ツールチェーンテンプレートが作成されます。を使用してプロジェクト AWS CLI を作成する場合は、ツールチェーンリソースを作成するツールチェーンテンプレートを作成します。

完全なツールチェーンを作成するには、次の推奨リソースが必要です：

1. ソースコードを保存する CodeCommit または GitHub リポジトリ。

2. リポジトリへの変更をリッスンするよう設定されている CodePipeline パイプライン。

   a. CodeBuild を使用してユニットテストまたは統合テストを使用する場合は、ビルドステージをパイプラインに追加してビルドアーティファクトを追加することをお勧めします。

   b. CodeDeploy または を使用してビルドアーティファクトとソースコードをランタイムインフラストラクチャ CloudFormation にデプロイするデプロイステージをパイプラインに追加することをお勧めします。

> **Note**
>
> CodePipeline では、2 つ以上のステージがパイプラインに必要であり、最初のステージはソースステージにする必要があるため、ビルドステージまたはデプロイステージを 2 番目のステージとして追加します。

AWS CodeStar ツールチェーンは CloudFormation テンプレートとして定義されます。

このタスクで説明しているチュートリアルおよびサンプルリソースの設定については、「チュートリアル: AWS CodeStar を使用して でプロジェクトを作成する AWS CLI」を参照してください。

前提条件:

プロジェクトを作成する際、入力ファイルで次のパラメータを指定します。以下が指定されていない場合、 は空のプロジェクト AWS CodeStar を作成します。

- ソースコード。このパラメータがリクエストに含まれている場合は、ツールチェーンテンプレートも含む必要があります。
  - ソースコードには、プロジェクトの実行に必要なアプリケーションコードを含む必要があります。
  - ソースコードには、必要な設定ファイル (例: CodeBuild プロジェクトの場合は buildspec.yml、CodeDeploy のデプロイの場合は appspec.yml) を含む必要があります。
  - README や template.yml などのオプション項目を、ツールチェーン以外の AWS リソースのソースコードに含めることができます。
- ツールチェーンテンプレート。ツールチェーンテンプレートは、プロジェクトで管理される AWS リソースと IAM ロールをプロビジョニングします。
- ソースの場所。プロジェクトのソースコードおよびツールチェーンテンプレートを指定する場合は、場所を指定する必要があります。ソースファイルおよびツールチェーンテンプレートを

Amazon S3 バケットにアップロードします。 AWS CodeStar はファイルを取得後、それを使用してプロジェクトを作成します。

> **Important**
>
> で優先 AWS リージョンを設定してください AWS CLI。プロジェクトは、 で設定された AWS リージョンに作成されます AWS CLI。

1. create-project コマンドを実行し、`--generate-cli-skeleton` パラメータを含めます。

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

JSON 形式のデータが出力に表示されます。 AWS CLI がインストールされているローカルコンピュータまたはインスタンス上の場所にある ファイル (など*input.json*) にデータをコピーします。コピーされたデータを次のように変更して、結果を保存します。

```
{
    "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"
    }
}
```

以下に置き換えます:

- *project-name*: 必須。この AWS CodeStar プロジェクトのフレンドリ名。
- *project-id*: 必須。このプロジェクトの AWS CodeStar プロジェクト ID。

> **Note**
>
> プロジェクト作成時、一意のプロジェクト ID が必要です。既に存在するプロジェクト ID を使用して入力ファイルを送信すると、エラーが表示されます。

- *##*: オプション。この AWS CodeStar プロジェクトの説明。
- *sourceCode*: オプション。プロジェクト用に指定されたソースコードの設定情報。現在は、単一の sourceCode オブジェクトのみサポートされています。各sourceCodeオブジェクトには、ソースコードが によって取得される場所 AWS CodeStar と、ソースコードが入力された送信先に関する情報が含まれています。
  - *source*: 必須。これにより、ソースコードをアップロードした場所が定義されます。サポートされている唯一のソースは Amazon S3 です。 はソースコード AWS CodeStar を取得し、プロジェクトの作成後にリポジトリに含めます。

- *S3*: オプション。ソースコードの Amazon S3 の場所。
  - *bucket-name*: ソースコードが含まれるバケット。
  - *bucket-key*: ソースコードを含む .zip ファイル (例: `src.zip`) を指すバケットのプリフィックスとオブジェクトキー。
- *###*: オプション。プロジェクト作成時にソースコードが追加される送信先の場所。ソースコードの送信先として、CodeCommit および GitHub がサポートされています。

  これらの 2 つのオプションのうちいずれかのみ指定することができます :

  - *codeCommit*: 必要な属性は、ソースコードを含む必要のある CodeCommit リポジトリの名前のみです。このリポジトリは、ツールチェーンテンプレートに含まれている必要があります。

    > **Note**
    >
    > CodeCommit では、ツールチェーンスタックで定義されているリポジトリの名前を指定する必要があります。 AWS CodeStar は、Amazon S3 で指定したソースコードを使用してこのリポジトリを初期化します。

  - *gitHub*: このオブジェクトは、GitHub リポジトリを作成し、ソースコードと連携するために必要な情報を表します。GitHub リポジトリを選択した場合は、以下の値が必要になります。

    > **Note**
    >
    > GitHub では、既存の GitHub リポジトリを指定することはできません。 はリポジトリ AWS CodeStar を作成し、このリポジトリに Amazon S3 にアップロードしたソースコードを入力します。 は、次の情報 AWS CodeStar を使用して GitHub にリポジトリを作成します。

    - *name*: 必須。GitHub リポジトリの名前。
    - *description*: 必須。GitHub リポジトリの説明。
    - *type*: 必須。GitHub リポジトリのタイプ。有効な値は、[User] (ユーザー)または [Organization] (組織)です。
    - *owner*: 必須。リポジトリの所有者を表す GitHub ユーザー の名前。リポジトリの所有者が GitHub 組織の場合は、組織名を入力します。

- *privateRepository*: 必須。このリポジトリをプライベートにするか公開にするか。有効な値は、true または false です。
- *issuesEnabled*: 必須。このリポジトリで、GitHub の課題を有効にするかどうか。有効な値は、true または false です。
- *[token]* (トークン) : オプション。これは、 AWS CodeStar が GitHub アカウントにアクセスするために使用する個人用アクセストークンです。このトークンには、スコープ repo、user、admin:repo_hook を含む必要があります。GitHub からの個人用アクセストークンを取得するには、GitHub ウェブサイトの[Creating a Personal Access Token for the Command Line] (コマンドライン用のパーソナルアクセストークンの作成) を参照してください。

  > **Note**
  >
  > CLI を使用して GitHub ソースリポジトリでプロジェクトを作成する場合、 はトークン AWS CodeStar を使用して OAuth アプリを介してリポジトリにアクセスします。コンソールを使用して GitHub ソースリポジトリでプロジェクトを作成する場合、 は GitHub アプリを使用してリポジトリにアクセスする接続リソース AWS CodeStar を使用します。

- *toolchain*: プロジェクトの作成時に設定される CI/CD ツールチェーンに関する情報。ツールチェーンテンプレートをアップロードした場所が含まれています。テンプレートによって、ツールチェーンリソースが含まれる CloudFormation スタックが作成されます。 これには、 が参照 CloudFormation するパラメータオーバーライドと、スタックの作成に使用されるロールも含まれます。 AWS CodeStar はテンプレートを取得し、CloudFormation を使用してテンプレートを実行します。
  - *source*: 必須。ツールチェーンテンプレートの場所です。Amazon S3 のみ、ソースの場所としてサポートされています。
    - *S3*: オプション。ツールチェーンテンプレートをアップロードした Amazon S3 の場所。
      - *bucket-name* : Amazon S3 バケットの名前。
      - *bucket-key*: ツールチェーンテンプレートを含む .yml ファイルまたは .json ファイル (例: `files/toolchain.yml`) を指すバケットのプリフィックスとオブジェクトキー。

- *stackParameters*: オプション。 CloudFormationに渡されるキーと値のペアが含まれます。これらはパラメータです (ある場合)。ツールチェーンテンプレートは参照用にセットアップされます。
- *role*: オプション。アカウントでツールチェーンリソースを作成するために使用されるロール。このロールは次を満たしている必要があります：
  - ロールが指定されていない場合、ツールチェーンが AWS CodeStar クイックスタートテンプレートである場合、 はアカウント用に作成されたデフォルトのサービスロール AWS CodeStar を使用します。サービスロールがアカウントに存在しない場合は、新たに作成することができます。詳細については、ステップ 2: AWS CodeStar サービスロールを作成する を参照してください。
  - カスタムツールチェーンテンプレートをアップロードして使用している場合は、ロールを指定する必要があります。 AWS CodeStar のサービスロールとポリシーステートメントに基づいてロールを作成できます。 このポリシーステートメントの例については、「AWSCodeStarServiceRole ポリシー」を参照してください。
- *tags*: オプション。 AWS CodeStar プロジェクトにアタッチされたタグ。

> **Note**
>
> これらのタグは、プロジェクトに含まれるリソースに添付されていません。

2. 保存したばかりのファイルがあるディレクトリに移動し、create-project コマンドをもう一度実行します。`--cli-input-json` パラメータを指定します。

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

3. 成功すると、次のようなデータが出力に表示されます：

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

- この出力には、新しいプロジェクトに関する情報が含まれています：
  - `id` 値はプロジェクト ID を表します。
  - `arn` 値は、プロジェクトの ARN を表します。

4. プロジェクトの作成ステータスを確認するには、describe-project コマンドを使用します。--id パラメータを指定します。

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

次のようなデータが出力に表示されます。

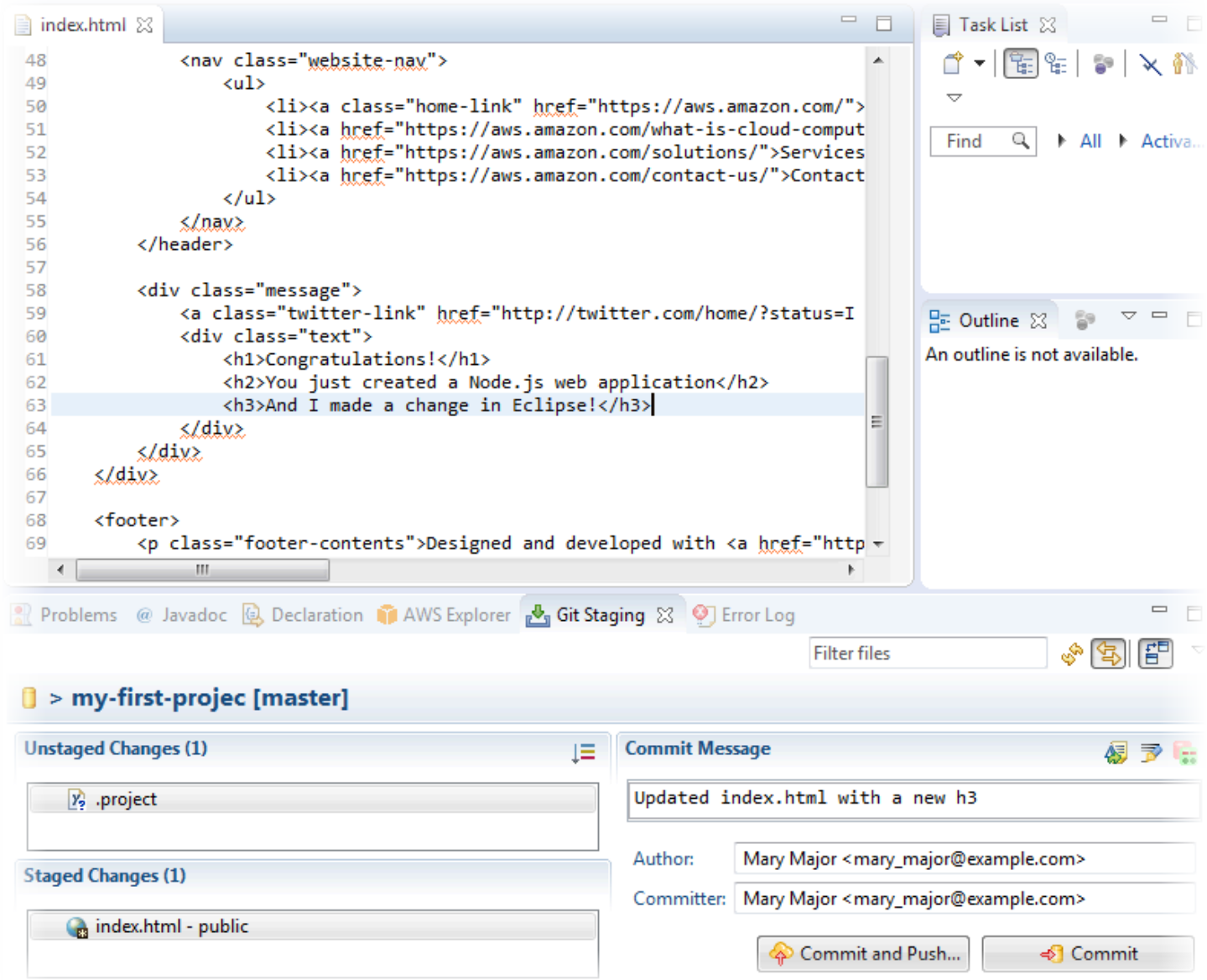
```
{
    "name": "MyProject",
    "id": "myproject",
    "arn": "arn:aws:codestar:us-east-1:account_ID:project/myproject",
    "description": "",
    "createdTimeStamp": 1539700079.472,
    "stackId": "arn:aws:cloudformation:us-east-1:account_ID:stack/awscodestar-
myproject/stack-ID",
    "status":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

- この出力には、新しいプロジェクトに関する情報が含まれています :
  - state 値は、プロジェクトの作成ステータス (例: CreateInProgress または CreateComplete) を表します。

プロジェクトが作成される間、コマンドライン またはお好みの IDE からプロジェクトリポジトリに [add team members] (チームメンバーの追加)、または [configure access] (アクセスの設定) を行うことができます。

で IDE を使用する AWS CodeStar

IDE を と統合すると AWS CodeStar、引き続き任意の環境でコードを記述して開発できます。コードのコミットとプッシュを行うたびに、変更が AWS CodeStar プロジェクトに含まれます。



トピック

- AWS Cloud9 で を使用する AWS CodeStar
- で Eclipse を使用する AWS CodeStar
- で Visual Studio を使用する AWS CodeStar

AWS Cloud9 で を使用する AWS CodeStar

を使用して AWS Cloud9 、 AWS CodeStar プロジェクトでコードの変更やソフトウェアの開発を行うことができます。 AWS Cloud9 は、ウェブブラウザからアクセスできるオンライン IDE です。この IDE では、リッチなコード編集エクスペリエンスを実現しており、複数のプログラミン

グ言語、ランタイムデバッガ、組み込みターミナルがサポートされています。バックグラウンドでは、Amazon EC2 インスタンスは AWS Cloud9 開発環境をホストします。この環境は、IDE AWS Cloud9 と AWS CodeStar プロジェクトのコードファイルへのアクセスを提供します。詳細については、AWS Cloud9 ユーザーガイドをご参照ください。

AWS CodeStar コンソールまたは AWS Cloud9 コンソールを使用して、CodeCommit にコードを保存するプロジェクト AWS Cloud9 の開発環境を作成できます。GitHub にコードを保存する AWS CodeStar プロジェクトでは、 AWS Cloud9 コンソールのみを使用できます。このトピックでは、両方のコンソールの使用方法について説明します。

を使用するには AWS Cloud9、以下が必要です。

- プロジェクトにチームメンバーとして追加された IAM ユーザー AWS CodeStar 。
- AWS CodeStar プロジェクトがソースコードを CodeCommit に保存する場合、IAM ユーザーの AWS 認証情報。

トピック

プロジェクトの AWS Cloud9 環境を作成する

AWS CodeStar プロジェクトの AWS Cloud9 開発環境を作成するには、次の手順に従います。

1. 新しいプロジェクトを作成する場合、プロジェクトの作成 の手順を行います。
2. AWS CodeStar コンソールでプロジェクトを開きます。ナビゲーションバーで、[IDE] を選択します。[Create environment] (環境の作成) を選択し、次のステップを実行します。

> **Important**
>
> プロジェクトが がサポートされ AWS Cloud9 ていない AWS リージョンにある場合、ナビゲーションバーの IDE タブに AWS Cloud9 オプションは表示されません。

ただし、 AWS Cloud9 コンソールを使用して開発環境を作成し、新しい環境を開き、プロジェクトの AWS CodeCommit リポジトリに接続できます。次の手順をスキップして、「AWS Cloud9 ユーザーガイド」 の「環境を作成する」、「環境を開く」、「AWS CodeCommit サンプル」を参照してください。サポートされている AWS リージョンのリストについては、 AWS Cloud9の「」を参照してくださいAmazon Web Services 全般のリファレンス。

AWS Cloud9 環境の作成で、プロジェクトのデフォルトをカスタマイズします。

1. 環境をホストするように Amazon EC2 インスタンスのデフォルトのタイプを変更するには、[Instance type] (インスタンスタイプ)で、インスタンスタイプを選択します。
2. AWS Cloud9 は、 AWS アカウントの Amazon Virtual Private Cloud (Amazon VPC) を使用してインスタンスと通信します。 AWS アカウントで Amazon VPC がどのように設定されているかに応じて、次のいずれかを実行します。

アカウントに VPC があり、その VPC に 1 つ以上のサブネットがある	アカウントでデフォルト VPC AWS Cloud9 を使用する VPC は ですか？	VPC のサブネットが 1 つのみである	この操作を行います
いいえ	—	—	VPC が存在しない場合は、作成してください。[Network settings] (ネットワーク設定) を展開します。[Network(VPC)] (ネットワーク (VPC)) で、[Create VPC] (VPC の作成) を選択し、そのページの手順に従います。詳細については、「AWS Cloud9 ユーザーガイド」 の「 AWS Cloud9用のAmazon VPC の作成」を参照してください。 VPC が存在するがサブネットがない場合は、作成します。[Network settings] (ネットワーク設定) を展開します。[Network (VPC)] (ネットワーク (VPC)) で、[Create subnet] (サブネットの作成) を選択し、

アカウントに VPC があり、その VPC に 1 つ以上のサブネットがある	アカウントでデフォルト VPC AWS Cloud9 を使用する VPC は ですか？	VPC のサブネットが 1 つのみである	この操作を行います
			手順に従います。詳細については、AWS Cloud9 ユーザーガイド の 「AWS Cloud9用のサブネットの作成」 を参照してください。
あり	あり	あり	この手順のステップ 4 に進みます (単一のサブネットでデフォルトの VPC AWS Cloud9 を使用します)。
あり	はい	いいえ	[Subnet] (サブネット) で、 AWS Cloud9 で使用する、事前に選択されたデフォルト VPC のサブネットを選択します。
はい	いいえ	はい/いいえ	ネットワーク (VPC) AWS Cloud9 で、使用する VPC を選択します。Subnet で、その VPC AWS Cloud9 で使用するサブネットを選択します。

詳細については、「 AWS Cloud9 ユーザーガイド」のAWS Cloud9 「開発環境の Amazon VPC 設定」を参照してください。

3. [Environment name] (環境名) を入力し、オプションで [Environment description] (環境の説明) を追加します。

> **Note**
>
> 環境名はユーザーごとに一意である必要があります。

4. を使用していないときに が環境を AWS Cloud9 シャットダウンするデフォルトの期間を変更するには、コスト削減設定を展開し、設定を変更します。
5. [Create environment] (環境の作成) を選択します。

環境を開くには、「プロジェクトの AWS Cloud9 環境を開く」を参照してください。

以下のステップに従い、プロジェクトの環境を 2 つ以上作成します。例えば、ある環境を使用してコードの一部を処理し、別の環境を使用して異なる設定でコードの同じ部分を処理することができます。

プロジェクトの AWS Cloud9 環境を開く

AWS CodeStar プロジェクト用に作成した AWS Cloud9 開発環境を開くには、次の手順に従います。

1. AWS CodeStar コンソールでプロジェクトを開き、ナビゲーションバーで IDE を選択します。

> **Important**
>
> プロジェクトのソースコードが GitHub に保存されている場合は、ナビゲーションバーに [IDE] は表示されません。ただし、 AWS Cloud9 コンソールを使用して既存の環境を開くことができます。この手順の残りの手順をスキップして、「AWS Cloud9 ユーザーガイド」 の 「環境を開く」 およびで GitHub を使用する AWS Cloud9 を参照してください。

2. AWS Cloud9 環境または共有 AWS Cloud9 環境では、開く環境の Open IDE を選択します。

AWS Cloud9 IDE を使用して、プロジェクトの AWS CodeCommit リポジトリ内のコードの使用をすぐに開始できます。詳細については、「AWS Cloud9 ユーザーガイド」 の 環境ウィンドウ」、「エディター、タブ、ペイン」、および「ターミナル」、「AWS CodeCommit ユーザーガイド」 の 「基本的な Git コマンド」 を参照してください。

プロジェクトチームメンバーと AWS Cloud9 環境を共有する

AWS CodeStar プロジェクトの AWS Cloud9 開発環境を作成したら、プロジェクトチームメンバーを含む AWS アカウント全体の他のユーザーを招待して、同じ環境にアクセスできます。これは、2 人のプログラマーが交互にコーディングし、画面共有しながら同じコードに関するアドバイスを行うか、同じワークステーションに座ってペアプログラミングを行う場合に特に便利です。環境メンバーは、共有 AWS Cloud9 IDE を使用して、コードエディタで強調表示された各メンバーのコード変更を表示したり、コーディング中に他のメンバーとテキストチャットしたりできます。

チームメンバーをプロジェクトに追加しても、そのメンバーはプロジェクトの関連する AWS Cloud9 開発環境に自動的に参加することはできません。プロジェクトの環境にアクセスするようにプロジェ

クトチームメンバーを招待するには、正しい環境メンバーアクセスロールを決定し、 AWS 管理ポリシーをユーザーに適用して、ユーザーを環境に招待する必要があります。詳細については、「AWS Cloud9 ユーザーガイド」の「環境メンバーのアクセスロールについて」および「環境に IAM ユーザーを招待する」を参照してください。

プロジェクトの環境にアクセスできるようにプロジェクトチームメンバーを招待すると、 AWS CodeStar コンソールにそのチームメンバーへの環境が表示されます。環境は、プロジェクトの AWS CodeStar コンソールの IDE タブの共有環境リストに表示されます。このリストを表示するには、チームメンバーがコンソールでプロジェクトを開き、ナビゲーションバーの [IDE] を選択します。

> **Important**
>
> プロジェクトのソースコードが GitHub に保存されている場合は、ナビゲーションバーに [IDE] は表示されません。ただし、 AWS Cloud9 コンソールを使用して、プロジェクトチームメンバーを含む AWS アカウント全体の他のユーザーを 環境へのアクセスに招待できます。これを行うには、このガイドの「で GitHub を使用する AWS Cloud9」と「AWS Cloud9 ユーザーガイド」の「環境メンバーのアクセスロールについて」および「環境に IAM ユーザーを招待する」を参照してください。

また、環境にアクセスできるように、プロジェクトチームメンバーではないユーザーを招待することもできます。例えば、ユーザーはプロジェクトのコードを操作するが、プロジェクトの他の部分へアクセスできないようにすることができます。このタイプのユーザーを招待するには、「AWS Cloud9 ユーザーガイド」の「環境メンバーのアクセスロールについて」および「環境にIAM ユーザーを招待する」を参照してください。プロジェクトの環境にアクセスできるようにプロジェクトチームメンバーではないユーザーを招待すると、そのユーザーは、 AWS Cloud9 コンソールを使用して、環境にアクセスすることができます。詳細については、「AWS Cloud9 ユーザーガイド」 の 「環境を開く」 を参照してください。

プロジェクトから AWS Cloud9 環境を削除する

プロジェクトとそのすべての AWS リソースを から削除すると AWS CodeStar、 AWS CodeStar コンソールで作成された関連する AWS Cloud9 すべての開発環境も削除され、復元することはできません。開発環境は、プロジェクトを削除する必要なく、プロジェクトから削除することができます。

1. AWS CodeStar コンソールでプロジェクトを開き、ナビゲーションバーで IDE を選択します。

> **Important**
>
> プロジェクトのソースコードが GitHub に保存されている場合は、ナビゲーションバーに [IDE] は表示されません。ただし、 AWS Cloud9 コンソールを使用して開発環境を削除できます。この手順の残りの手順をスキップして、「AWS Cloud9 ユーザーガイド」の 「環境を削除する」 を参照してください。

2. [Cloud9 environments] (Cloud9 環境) で削除する環境を選択し、[Delete] (削除) を選択します。
3. 開発環境の削除を確認するため **`delete`** を入力し、[Delete] (削除) を選択します。

> **Warning**
>
> 削除した開発環境を復元することはできません。この環境でコミットされていないコードの変更はすべて、失われます。

で GitHub を使用する AWS Cloud9

ソースコードが GitHub に保存されている AWS CodeStar プロジェクトの場合、 AWS CodeStar コンソールは AWS Cloud9 開発環境の直接操作をサポートしていません。ただし、 AWS Cloud9 コンソールを使用して GitHub リポジトリのソースコードを操作できます。

1. AWS Cloud9 コンソールを使用して AWS Cloud9 開発環境を作成します。詳細については、「AWS Cloud9 ユーザーガイド」 の 「環境の作成」 を参照してください。
2. AWS Cloud9 コンソールを使用して開発環境を開きます。詳細については、「AWS Cloud9 ユーザーガイド」 の 「環境を開く」 を参照してください。
3. IDE で、ターミナルセッションを使用して GitHub リポジトリに接続します (クローニングと呼ばれるプロセス)。ターミナルセッションが実行されていない場合は、IDE のメニューバーで [Window, New Terminal](ウインドウ、新しいターミナル) を選択します。GitHub リポジトリのクローン作成に使用するコマンドについては、GitHub のヘルプウェブサイトの [Cloning a Repository] (リポジトリのクローン作成) を参照してください。

   GitHub リポジトリのメインページに移動するには、 AWS CodeStar コンソールでプロジェクトを開き、サイドナビゲーションバーでコードを選択します。

4. IDE の [Environment] (環境) ウィンドウとエディタタブを使用して、コードを表示、変更、保存します。詳細については、「AWS Cloud9 ユーザーガイド」 の 「環境」ウィンドウ および エディター、タブ、ペイン を参照してください。
5. IDE のターミナルセッションの Git を使用して、コードの変更をリポジトリにプッシュし、リポジトリの他のコードの変更を定期的にリポジトリからプルできます。詳細については、GitHub ヘルプウェブサイトの [Pushing to a Remote Repository] (リモートリポジトリへのプッシュ) および [Fetching a Remote Repository] (リモートリポジトリの取得) を参照してください。Git コマンドについては、GitHub のヘルプウェブサイトの 「Git Cheatsheet」 を参照してください。

> **Note**
>
> リポジトリからコードをプッシュまたはプルするたびに GitHub のサインイン認証情報の入力を求めるように Git に指示する場合は、認証情報ヘルパーを使用できます。詳細については、GitHub Help ウェブサイトの [Caching Your GitHub Password in Git] (Git に GitHub パスワードをキャッシュする) を参照してください。

その他のリソース

の使用の詳細については AWS Cloud9、 AWS Cloud9 ユーザーガイドの以下を参照してください。

- チュートリアル
- 環境を使用する
- IDE を操作する
- サンプル

で Eclipse を使用する AWS CodeStar

Eclipse を使用してコードを変更し、 AWS CodeStar プロジェクトでソフトウェアを開発できます。Eclipse で AWS CodeStar プロジェクトコードを編集し、変更をコミットして AWS CodeStar プロジェクトのソースリポジトリにプッシュできます。

> **Note**
>
> このトピックの情報は、ソースコードを CodeCommit に保存している AWS CodeStar プロジェクトにのみ適用されます。 AWS CodeStar プロジェクトがソースコードを GitHub に保

存している場合は、EGit for Eclipse などのツールを使用できます。詳細については、EGit ウェブサイトの [EGit Documentation] (EGit ドキュメント) を参照してください。

AWS CodeStar プロジェクトがソースコードを CodeCommit に保存する場合は、 がサポート AWS Toolkit for Eclipse する のバージョンをインストールする必要があります AWS CodeStar。また、所有者または寄稿者ロールを持つ AWS CodeStar プロジェクトチームのメンバーである必要があります。

Eclipse を使用するには、以下の条件を満たす必要があります：

- チームメンバーとして AWS CodeStar プロジェクトに追加された IAM ユーザー。
- AWS CodeStar プロジェクトがソースコードを CodeCommit に保存する場合、IAM ユーザーの Git 認証情報 (サインイン認証情報) 。
- Eclipse と をローカルコンピュータ AWS Toolkit for Eclipse にインストールするための十分なアクセス許可。

トピック

ステップ 1: をインストールする AWS Toolkit for Eclipse

Toolkit for Eclipse は、Eclipse に追加できるソフトウェアパッケージです。Eclipse の他のソフトウェアパッケージと同じ方法でインストールおよび管理されます。 AWS CodeStar ツールキットは Toolkit for Eclipse の一部として含まれています。

AWS CodeStar モジュールを使用して Toolkit for Eclipse をインストールするには

1. Eclipse をローカルコンピュータにインストールします。サポートされている Eclipse のバージョンには、Luna、Mars、Neon があります。
2. Toolkit for Eclipse をダウンロードしてインストールします。詳細については、「AWS Toolkit for Eclipse 入門ガイド」 を参照してください。
3. Eclipse で [Help] (ヘルプ) を選択してから、[Install New Software] (新しいソフトウェアのインストール) を選択します。

4. [Available Software] (利用可能なソフトウェア) で、[Add] (追加) を選択します。
5. [Add Repository] (リポジトリの追加) で、[Archive] (アーカイブ) を選択し、.zip ファイルを保存した場所を参照して、ファイルを開きます。[Name] (名前) を空欄にし、[OK] を選択します。
6. [利用可能なソフトウェア] で、[すべて選択] を選択して、[AWS コア管理ツール] と [開発者用ツール] の両方を選択し、[次へ] を選択します。
7. [Install Details] (インストールの詳細) で、[Next] (次へ) を選択します。
8. [Review Licenses] (ライセンスの確認) で、ライセンス契約を確認します。[I accept the terms of the license agreement] (ライセンス契約の条項に同意します) を選択し、[Finish] (完了) を選択します。Eclipse を再起動します。

ステップ 2: AWS CodeStar プロジェクトを Eclipse にインポートする

Toolkit for Eclipse をインストールしたら、 AWS CodeStar プロジェクトをインポートし、IDE からコードを編集、コミット、プッシュできます。

> **Note**
>
> Eclipse の 1 つのワークスペースに複数の AWS CodeStar プロジェクトを追加できますが、あるプロジェクトから別のプロジェクトに変更する場合は、プロジェクトの認証情報を更新する必要があります。

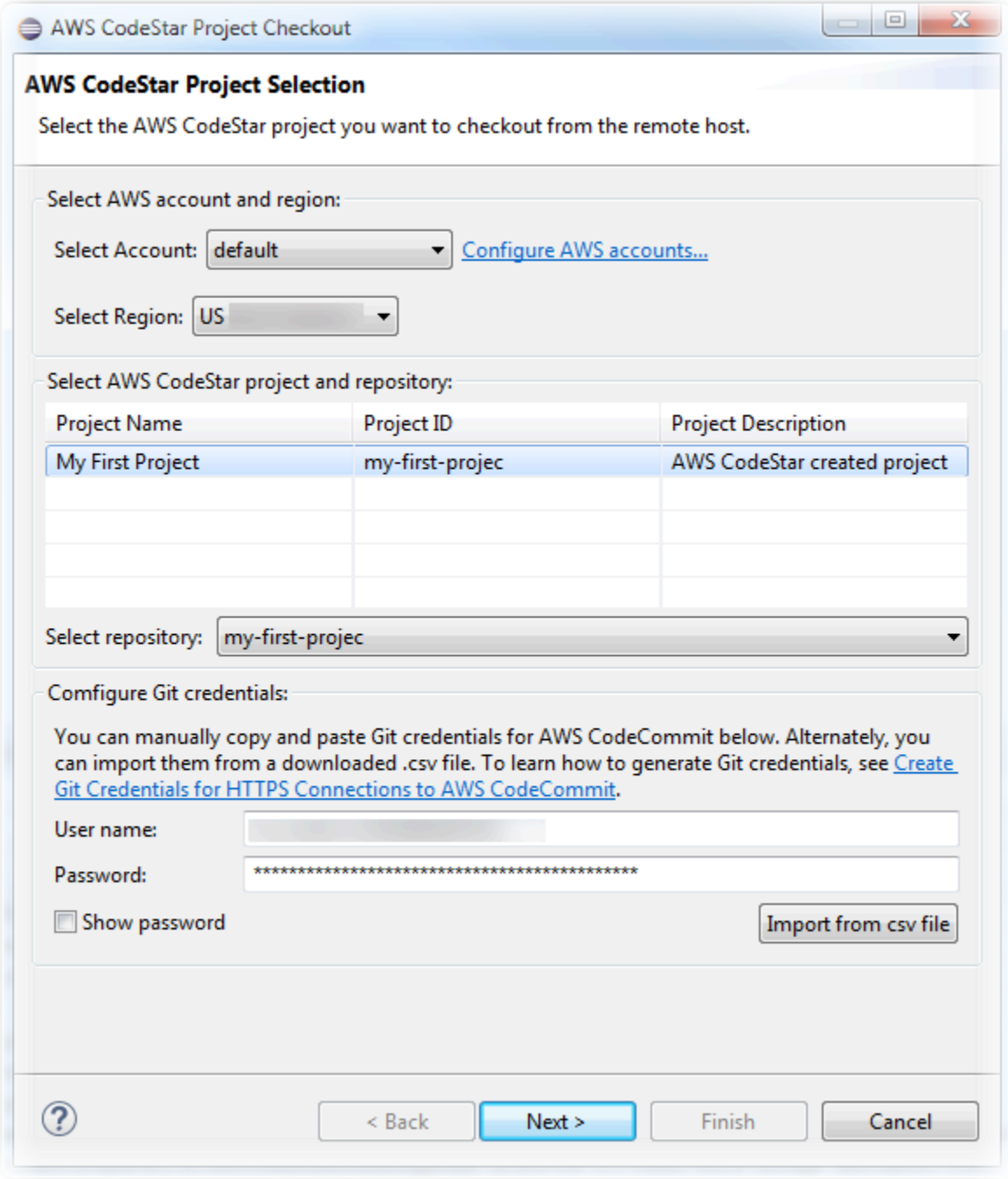
AWS CodeStar プロジェクトをインポートするには

1. AWS メニューから、 AWS CodeStar プロジェクトをインポートを選択します。または、[File] (ファイル)、[Import] (インポート) の順に選択します。Select で AWS を展開し、 AWS CodeStar Project を選択します。

   [Next (次へ)] を選択します。
2. AWS CodeStar プロジェクト選択で、 AWS プロファイルと AWS CodeStar プロジェクトがホストされている AWS リージョンを選択します。コンピュータにアクセスキーとシークレットキーで AWS プロファイルを設定していない場合は、 AWS アカウントの設定を選択し、手順に従います。

   Select AWS CodeStar project and repository で、プロジェクトを選択します AWS CodeStar 。[Git 認証情報の設定] に、プロジェクトのリポジトリにアクセスするために生成し

たユーザー名とパスワードを入力します。(git 認証情報がない場合は、「ご利用開始にあたって」を参照してください。) [Next (次へ)] を選択します。



3. プロジェクトのリポジトリのすべてのブランチがデフォルトで選択されます。1 つまたは複数のブランチをインポートしたくない場合は、ボックスをクリアして、[Next] (次へ) を選択します。
4. [Local Destination] (ローカルの作成先) で、インポートウィザードがコンピュータ上でローカルリポジトリを作成する場所を選択し、[Finish] (完了) を選択します。

5. Project Explorer で、プロジェクトツリーを展開して AWS CodeStar プロジェクト内のファイルを参照します。

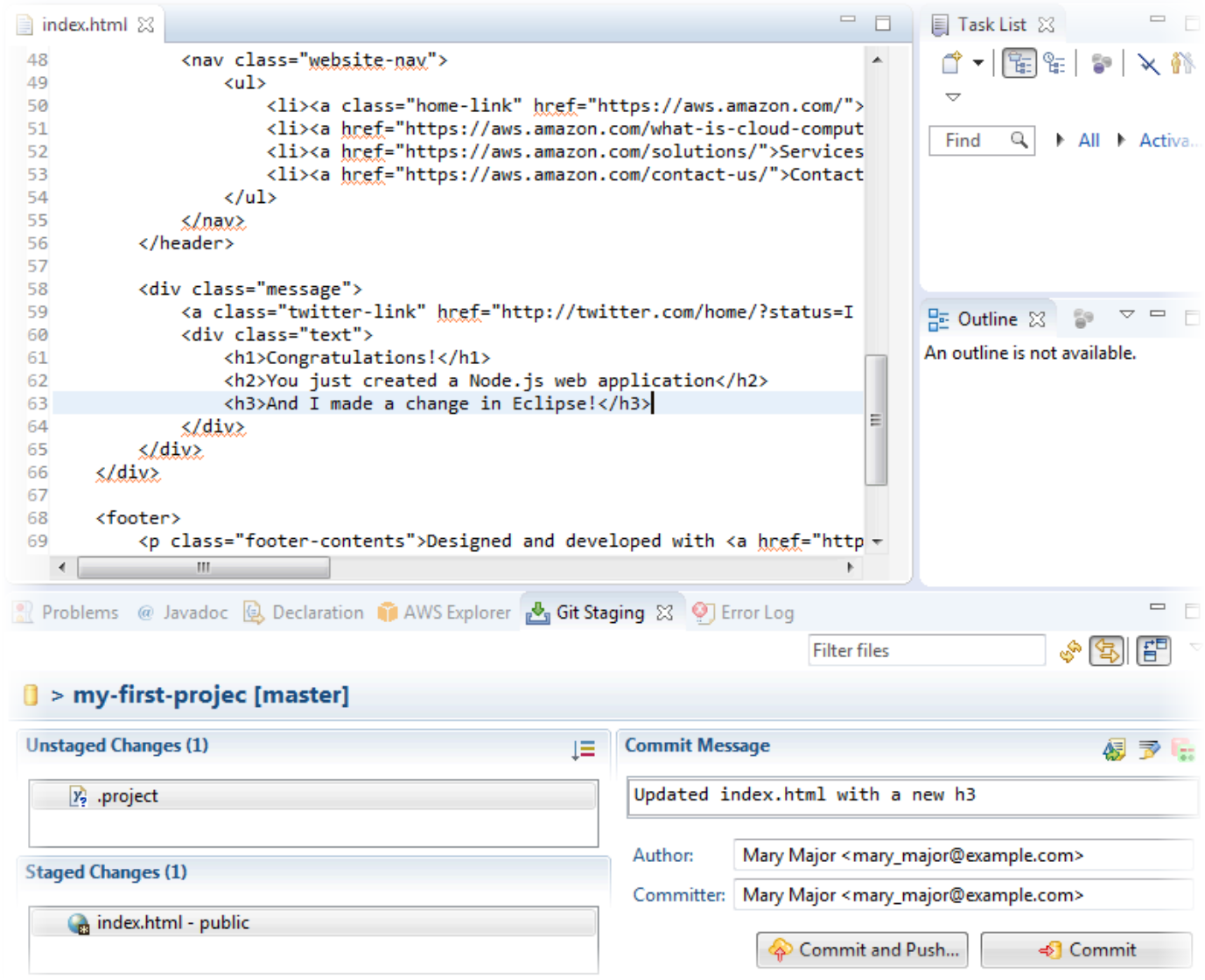
ステップ 3: Eclipse で AWS CodeStar プロジェクトコードを編集する

AWS CodeStar プロジェクトを Eclipse ワークスペースにインポートしたら、プロジェクトのコードを編集して変更を保存し、コードをコミットしてプロジェクトのソースリポジトリにプッシュできます。これは Eclipse 用の EGit プラグインを使用する Git リポジトリと同じプロセスです。詳細については、Eclipse ウェブサイトの「EGit ユーザーガイド」を参照してください。

プロジェクトコードを編集し、 AWS CodeStar プロジェクトのソースリポジトリに最初のコミットを行うには

1. Project Explorer で、プロジェクトツリーを展開して AWS CodeStar プロジェクト内のファイルを参照します。
2. 1 つまたは複数のコードファイルを編集し、変更を保存します。
3. 変更をコミットする準備ができたら、そのファイルのコンテキストメニューを開き、[Team] (チーム)、[Commit] (コミット) の順に選択します。

   プロジェクトビューで [Git Staging] (Git をステージ) ウィンドウが既に開いている場合は、このステップをスキップします。
4. [Git Staging] (Git をステージ) で、変更されたファイルを [Staged Changes] (ステージングされた変更) に移動して変更をステージします。[Commit Message] (コミットメッセージ) にコミットメッセージを入力し、[Commit and Push] (コミットとプッシュ) を選択します。



コード変更のデプロイを表示するには、プロジェクトのダッシュボードに戻ります。詳細については、「ステップ 3: プロジェクトを表示する」を参照してください。

で Visual Studio を使用する AWS CodeStar

Visual Studio を使用してコードを変更し、 AWS CodeStar プロジェクトでソフトウェアを開発できます。

> **Note**
>
> Visual Studio for Mac は AWS Toolkit をサポートしていないため、 では使用できません AWS CodeStar。

このトピックの情報は、ソースコードを CodeCommit に保存している AWS CodeStar プロジェクトにのみ適用されます。 AWS CodeStar プロジェクトがソースコードを GitHub に保存している場合は、GitHub Extension for Visual Studio などのツールを使用できます。詳細については、GitHub Extension for Visual Studio ウェブサイトの [Overview] (概要) ページ、および GitHub ウェブサイトの [Getting Started with GitHub for Visual Studio] (GitHub for Visual Studio 入門) を参照してください。

Visual Studio を使用して AWS CodeStar プロジェクトのソースリポジトリ内のコードを編集するには、 がサポート AWS Toolkit for Visual Studio する のバージョンをインストールする必要があります AWS CodeStar。所有者または寄稿者のロールを持つ AWS CodeStar プロジェクトチームのメンバーでなければなりません。

Visual Studio を使用するには、以下の条件を満たす必要があります:

- チームメンバーとして AWS CodeStar プロジェクトに追加された IAM ユーザー。
- AWS IAM ユーザーの 認証情報 (アクセスキーやシークレットキーなど) 。
- Visual Studio と をローカルコンピュータ AWS Toolkit for Visual Studio にインストールするための十分なアクセス許可。

Toolkit for Visual Studio は、Visual Studio に追加できるソフトウェアパッケージです。Visual Studio の他のソフトウェアパッケージと同じ方法でインストールおよび管理されます。

AWS CodeStar モジュールを使用して Toolkit for Visual Studio をインストールし、プロジェクトリポジトリへのアクセスを設定するには

1. ローカルコンピュータに Visual Studio をインストールします。
2. Toolkit for Visual Studio をダウンロードしてインストールし、.zip ファイルをローカルフォルダまたはディレクトリに保存します。「開始方法 AWS Toolkit for Visual Studio」ページで、 AWS 認証情報を入力またはインポートし、保存して閉じるを選択します。
3. Visual Studio で、[Team Explorer] (チームエクスプローラー) を開きます。[Hosted Service Providers] (ホストされているサービスプロバイダー) で、[CodeCommit] を検索し、[Connect] (接続) を選択します。
4. [Manage Connections] (接続を管理)で、[Clone] (クローン) を選択します。プロジェクトのリポジトリとそのリポジトリのクローン作成先のローカルコンピュータのフォルダを選択し、[OK] を選択します。

5. Git 認証情報を作成するように求められたら、[Yes] (はい) を選択します。ツールキットは、ユーザーに代わって認証情報を作成しようとします。安全な場所に認証情報ファイルを保存します。これは、これらの認証情報を保存する必要がある唯一の機会です。ツールキットがユーザーの代わりに認証情報を作成できない場合、または [No] を選択した場合は、独自の Git 認証情報を作成して提供する必要があります。詳細については、「変更をコミットするようコンピュータを設定するには (IAM ユーザー)」を参照するか、オンラインの指示に従ってください。

   プロジェクトのクローン作成が完了すると、Visual Studio でコードを編集し、プロジェクトのリポジトリへの変更を CodeCommit でコミットしてプッシュする準備が整います。

プロジェクトの AWS リソース AWS CodeStar を変更する

でプロジェクトを作成したら AWS CodeStar、 がプロジェクト AWS CodeStar に追加する AWS リソースのデフォルトセットを変更できます。

サポートされているリソースの変更

次の表に、 プロジェクトで AWS CodeStar サポートされているデフォルト AWS リソースの変更を示します。

変更	メモ
ステージを に追加します AWS CodePipeline。	「ステージを に追加する AWS CodePipeline」を参照してください。
Elastic Beanstalk 環境設定を変更します。	「AWS Elastic Beanstalk 環境設定を変更する」を参照してください。
Amazon API Gateway で AWS Lambda 関数のコードまたは設定を変更する。	「ソースコードで AWS Lambda 関数を変更する」を参照してください。
AWS Lambda プロジェクトにリソースを追加し、新しいリソースを作成してアクセスするためのアクセス許可を展開します。	「リソースをプロジェクトに追加する」を参照してください。
AWS Lambda 関数の CodeDeploy を使用してトラフィックシフトを追加します。	「AWS Lambda プロジェクトのトラフィックを移行する」を参照してください。

変更	メモ
AWS X-Ray サポートの追加	「プロジェクトのトレースを有効にする」を参照してください。
プロジェクトの buildspec.yml ファイルを編集して、 AWS CodeBuild が実行するユニットテストビルドフェーズを追加します。	サーバーレスプロジェクトのチュートリアルの「ステップ 7: ウェブサービスにユニットテストを追加する」を参照してください。
独自の IAM ロールをプロジェクトに追加します。	「IAM ロールをプロジェクトに追加する」を参照してください。
IAM ロールの定義の変更	アプリケーションスタックで定義されているロールの場合。ツールチェーンまたは CloudFormation スタックで定義されているロールを変更することはできません。
Lambda プロジェクトを変更してエンドポイントを追加します。	
EC2 プロジェクトを変更してエンドポイントを追加します。	
Elastic Beanstalk プロジェクトを変更してエンドポイントを追加します。	
プロジェクトを編集し、Prod ステージとエンドポイントを追加します。	「Prod ステージとエンドポイントをプロジェクトに追加する」を参照してください。
AWS CodeStar プロジェクトで SSM パラメータを安全に使用します。	「the section called “AWS CodeStar プロジェクトで SSM パラメータを安全に使用する”」を参照してください。

以下の変更はサポートされていません。

- 別のデプロイターゲットに切り替えます (たとえば、 の代わりに に AWS Elastic Beanstalk デプロイします AWS CodeDeploy) 。
- フレンドリウェブエンドポイント名を追加します。

- CodeCommit リポジトリ名を変更します (CodeCommit に接続された AWS CodeStar プロジェクトの場合) 。
- GitHub に接続されている AWS CodeStar プロジェクトの場合は、GitHub リポジトリを切断し、そのプロジェクトにリポジトリを再接続するか、他のリポジトリをそのプロジェクトに接続します。パイプラインの [ソース] ステージで、CodePipeline コンソール (AWS CodeStar コンソールではない) を使用して、GitHub を切断して再接続することができます。ただし、[ソース] ステージを別の GitHub リポジトリに再接続すると、プロジェクトの AWS CodeStar ダッシュボードの [リポジトリ] および [問題] タイルの情報が間違っているか古くなっている場合があります。GitHub リポジトリを切断しても、そのリポジトリの情報はコミット履歴から削除されず、GitHub は AWS CodeStar プロジェクトダッシュボードのタイルを発行します。この情報を削除するには、GitHub ウェブサイトを使用して、 AWS CodeStar プロジェクトから GitHub へのアクセスを無効にします。アクセスを取り消すには、GitHub ウェブサイトで、GitHub アカウントプロファイルの設定ページの [Authorized OAuth Apps] (許可されたOAuth Apps) セクションを使用します。
- CodeCommit リポジトリ (CodeCommit に接続された AWS CodeStar プロジェクトの場合) CodeCommit を切断し、リポジトリをそのプロジェクトに再接続するか、他のリポジトリをそのプロジェクトに接続します。

ステージを に追加する AWS CodePipeline

プロジェクトで が AWS CodeStar 作成するパイプラインに新しいステージを追加できます。詳細については、「AWS CodePipeline ユーザーガイド」の「AWS CodePipelineでパイプラインを編集する」を参照してください。

> **Note**
>
> 新しいステージが によって作成 AWS CodeStar されなかった AWS リソースに依存する場合、パイプラインが中断される可能性があります。これは、 用に が AWS CodeStar 作成した IAM ロールが、デフォルトでこれらのリソースにアクセスできない AWS CodePipeline 可能性があるためです。
> が作成 AWS CodeStar しなかった AWS リソース AWS CodePipeline へのアクセスを許可しようとするには、 が AWS CodeStar 作成した IAM ロールを変更することができます。これはサポートされていません。プロジェクトで定期的に更新チェックを実行すると、 AWS CodeStar が IAM ロールの変更を削除する可能性があるためです。

AWS Elastic Beanstalk 環境設定を変更する

プロジェクトで が AWS CodeStar 作成する Elastic Beanstalk 環境の設定を変更できます。たとえば、 AWS CodeStar プロジェクトのデフォルトの Elastic Beanstalk 環境を単一インスタンスからロードバランシングに変更できます。これを行うには、プロジェクトのリポジトリ内の `template.yml` ファイルを編集します。プロジェクトのワーカーロールのアクセス許可を変更することが必要になる場合もあります。テンプレートの変更をプッシュ AWS CodeStar し、リソースを CloudFormation プロビジョニングした後。

`template.yml` ファイルの編集方法については、「Template.yml ファイルを使用してアプリケーションリソースを変更する」を参照してください。Elastic Beanstalk 環境の詳細については、「AWS Elastic Beanstalk デベロッパーガイド」の「AWS Elastic Beanstalk 環境マネジメントコンソール」を参照してください。

ソースコードで AWS Lambda 関数を変更する

がプロジェクトで AWS CodeStar 作成する Lambda 関数、またはその IAM ロールまたは API Gateway API のコードまたは設定を変更できます。これを行うには、プロジェクトの CodeCommit リポジトリの `template.yaml` ファイルとともに Serverless Application Model (AWS SAM) を使用する AWS ことをお勧めします。この `template.yaml` ファイルは、関数の名前、ハンドラ、ランタイム、IAM ロール、および API Gateway の API を定義します。詳細については、GitHub ウェブサイトのAWS 「SAM を使用してサーバーレスアプリケーションを作成する方法」を参照してください。

プロジェクトのトレースを有効にする

AWS X-Ray は、分散アプリケーションのパフォーマンス動作 (応答時間のレイテンシーなど) を分析するために使用できるトレースを提供します。 AWS CodeStar プロジェクトにトレースを追加したら、 AWS X-Ray コンソールを使用してアプリケーションビューと応答時間を表示できます。

> **Note**
>
> 以下のプロジェクトサポートの変更により作成された以下のプロジェクトでは、これらのステップを使用できます。
>
> - 任意の Lambda プロジェクト。

- 2018 年 8 月 3 日以降に作成された Amazon EC2 または Elastic Beanstalk プロジェクトの場合、 AWS CodeStar により、プロジェクトリポジトリに `/template.yml` ファイルがプロビジョニングされています。

各 AWS CodeStar テンプレートには、データベーステーブルや Lambda 関数など、アプリケーションの AWS ランタイム依存関係をモデル化する CloudFormation ファイルが含まれています。このファイルは、ファイル `/template.yml` のソースリポジトリに保存されています。

このファイルを変更してトレースを追加するには、 `Resources`セクションに AWS X-Ray リソースを追加します。次に、 がリソース CloudFormation を作成できるように、プロジェクトの IAM アクセス許可を変更します。テンプレート要素およびフォーマットについては、「AWS リソースタイプのリファレンス」を参照してください。

テンプレートをカスタマイズする大まかなステップを以下に示します。

1. ステップ 1: トレースに必要な IAM のワーカーロールを編集する
2. ステップ 2: トレース用に template.yml ファイルを変更する
3. ステップ 3: トレース用にテンプレートの変更をコミットおよびプッシュする
4. ステップ 4: トレース用の AWS CloudFormation スタック更新をモニタリングする

ステップ 1: トレースに必要な IAM のワーカーロールを編集する

ステップ 1 および 4 を実行するには、管理者ユーザーとしてサインインする必要があります。このステップでは、Lambda プロジェクトのアクセス許可を編集する例を示します。

> **Note**
>
> プロジェクトがアクセス許可の境界ポリシーでプロビジョニングされた場合は、このステップをスキップできます。
> 2018 年 12 月 6 日以降に作成されたプロジェクトの場合、 はアクセス許可の境界ポリシーを使用してプロジェクトを AWS CodeStar プロビジョニングしました。

1. にサインイン AWS マネジメントコンソール し、 AWS CodeStar コンソールを https://console.aws.amazon.com/codestar/://www.com で開きます。

2. プロジェクトを作成するか、`template.yml file` を含む既存のプロジェクトを選択して、[Project resources] (プロジェクトリソース) ページを開きます。
3. [Project Resources] (プロジェクトリソース) のリソースリストで、CodeStarWorker/Lambda ロール用に作成した IAM ロールを検索します。ルール名の形式は次のとおりです: `role/CodeStarWorker-`*`Project_name`*`-lambda-`*`Function_name`*。ロールの ARN を選択します。
4. ロールが IAM コンソールで開きます。[Attach policies] (ポリシーの添付) を選択します。`AWSXrayWriteOnlyAccess` ポリシーを検索し、その横にあるボックスを選択して、[Attach Policy] (ポリシーの添付) を選択します。

ステップ 2: トレース用に template.yml ファイルを変更する

1. AWS CodeStar コンソールを https://console.aws.amazon.com/codestar/://www.com で開きます。
2. サーバーレスプロジェクトを選択し、[Code] (コード) ページを開きます。リポジトリの最上位で、`template.yml` ファイルを検索して編集します。`Resources` で、リソースを `Properties` セクションに貼り付けます。

```
      Tracing: Active
```

この例では、変更後のテンプレートを示します。

```
Resources:
  GetHelloWorld:
    Type: AWS::Serverless::Function
    Properties:
      Handler: index.get
      Runtime: nodejs4.3
      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
```

ステップ 3: トレース用にテンプレートの変更をコミットおよびプッシュする

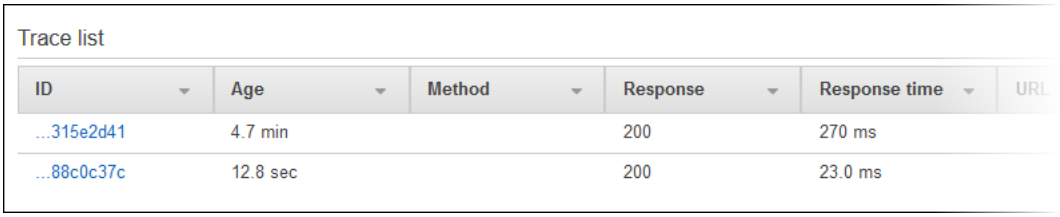
- `template.yml` ファイルの変更をコミットおよびプッシュします。

> **Note**
>
> これにより、パイプラインが開始されます。IAM アクセス許可を更新する前に変更をコミットすると、パイプラインが開始され、 AWS CloudFormation スタックの更新で エラーが発生し、スタックの更新がロールバックされます。この問題が発生した場合は、アクセス許可を修正し、パイプランを再起動します。

ステップ 4: トレース用の AWS CloudFormation スタック更新をモニタリングする

1. AWS CloudFormation スタックの更新は、プロジェクトのパイプラインが Deploy ステージを開始したときに開始されます。スタックの更新のステータスを確認するには、 AWS CodeStar ダッシュボードでパイプラインの AWS CloudFormation ステージを選択します。

   のスタック更新でエラー AWS CloudFormation が返された場合は、「」のトラブルシューティングガイドラインを参照してくださいAWS CloudFormation: アクセス許可の不足により、スタックの作成がロールバックされた。ワーカーロールのアクセス許可が不足している場合は、プロジェクトの Lambda ワーカーロールに添付されているポリシーを編集します。「ステップ 1: トレースに必要な IAM のワーカーロールを編集する」を参照してください。
2. パイプラインが正常に完了したことを確認するには、ダッシュボードを使用します。アプリケーションでトレースが有効になりました。
3. トレースが有効になったことを確認するには、Lambda コンソールで関数の詳細を表示します。
4. プロジェクトのアプリケーションエンドポイントを選択します。このアプリケーションとのやり取りがトレースされます。トレースの情報は、 AWS X-Ray コンソールで確認できます。



リソースをプロジェクトに追加する

すべてのプロジェクトの各 AWS CodeStar テンプレートには、データベーステーブルや Lambda 関数など、アプリケーションの AWS ランタイム依存関係をモデル化する CloudFormation ファイルが含まれています。これは、ファイル `/template.yml` のソースリポジトリに保存されています。

> **Note**
>
> 以下のプロジェクトサポートの変更により作成された以下のプロジェクトでは、これらのステップを使用できます。
>
> - 任意の Lambda プロジェクト。
> - 2018 年 8 月 3 日以降に作成された Amazon EC2 または Elastic Beanstalk プロジェクトの場合、 AWS CodeStar により、プロジェクトリポジトリに `/template.yml` ファイルがプロビジョニングされています。

このファイルは、 `Resources`セクションに CloudFormation リソースを追加することで変更できます。`template.yml` ファイルを変更すると、 AWS CodeStar と CloudFormation で新しいリソースをプロジェクトに追加できます。一部のリソースでは、他のアクセス許可をプロジェクトの CloudFormation ワーカーロールのポリシーに追加する必要があります。テンプレート要素およびフォーマットについては、「AWS リソースタイプのリファレンス」を参照してください。

プロジェクトに追加する必要のあるリソースを決定したら、テンプレートをカスタマイズするための大まかな手順に従って実行します。 CloudFormation リソースとその必要なプロパティのリストについては、AWS 「リソースタイプのリファレンス」を参照してください。

1. ステップ 1: IAM で CloudFormation ワーカーロールを編集する (任意)
2. ステップ 2: template.yml ファイルを変更する
3. ステップ 3: テンプレートの変更をコミットおよびプッシュする
4. ステップ 4: AWS CloudFormation スタック更新をモニタリングする
5. ステップ 5: インラインポリシーでリソースのアクセス許可を追加する

このセクションのステップを使用して、 AWS CodeStar プロジェクトテンプレートを変更してリソースを追加し、IAM でプロジェクトの CloudFormation ワーカーロールのアクセス許可を展開します。この例では、AWS::SQS::Queue リソースは、`template.yml` ファイルに追加されます。この変更により、 で Amazon Simple Queue Service キュー AWS CloudFormation をプロジェクトに追加する自動レスポンスが開始されます。

ステップ 1: IAM で CloudFormation ワーカーロールを編集する

ステップ 1 および 5 を実行するには、管理者ユーザーとしてサインインする必要があります。

> **Note**
>
> プロジェクトがアクセス許可の境界ポリシーでプロビジョニングされた場合は、このステップをスキップできます。
> 2018 年 12 月 6 日以降に作成されたプロジェクトの場合、 はアクセス許可の境界ポリシーを使用してプロジェクトを AWS CodeStar プロビジョニングしました。

1. にサインイン AWS マネジメントコンソール し、 AWS CodeStar コンソールを開きます。https://https://console.aws.amazon.com/codestar/.
2. プロジェクトを作成するか、`template.yml file` を含む既存のプロジェクトを選択して、[Project resources] (プロジェクトリソース) ページを開きます。
3. プロジェクトリソースで、リソースリストの CodeStarWorker/AWS CloudFormation role 用に作成された IAM ロールを見つけます。ルール名の形式は次のとおりです: `role/CodeStarWorker-`*`Project_name`*`-CloudFormation`。
4. ロールが IAM コンソールで開きます。[Permissions] (アクセス許可) タブの [Inline Policies] (インラインポリシー) で、サービスロールポリシーの列を開き、[Edit Policy] (ポリシーの編集) を選択します。
5. [JSON] タブを選択してポリシーを編集します。

   > **Note**
   >
   > ワーカーロールに添付されるポリシーは `CodeStarWorkerCloudFormationRolePolicy` です。

6. [JSON] フィールドで、`Statement` 要素に次のポリシーステートメントを追加します。

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

```
  ],
  "Effect": "Allow"
}
```

7. [Review policy] (ポリシーの確認) を選択して、ポリシーにエラーがないことを確認し、[Save changes] (変更の保存) を選択します。

ステップ 2: template.yml ファイルを変更する

1. AWS CodeStar コンソールを https://console.aws.amazon.com/codestar/.com で開きます。
2. サーバーレスプロジェクトを選択し、[Code] (コード) ページを開きます。リポジトリの最上位にある `template.yml` の場所を書き留めます。
3. リポジトリの `template.yml` ファイルを編集するには、IDE、コンソール、またはコマンドラインをローカルリポジトリで使用します。リソースを `Resources` セクションに貼り付けます。この例では、以下のテキストをコピーすると、`Resources` セクションが追加されます。

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

この例では、変更後のテンプレートを示します。

ステップ 3: テンプレートの変更をコミットおよびプッシュする

- ステップ 2 で保存した `template.yml` ファイルの変更をコミットおよびプッシュします。

> **Note**
>
> これにより、パイプラインが開始されます。IAM アクセス許可を更新する前に変更をコミットすると、パイプラインが起動し、 AWS CloudFormation スタックの更新にエラーが発生し、スタックの更新がロールバックされます。この問題が発生した場合は、アクセス許可を修正し、パイプランを再起動します。

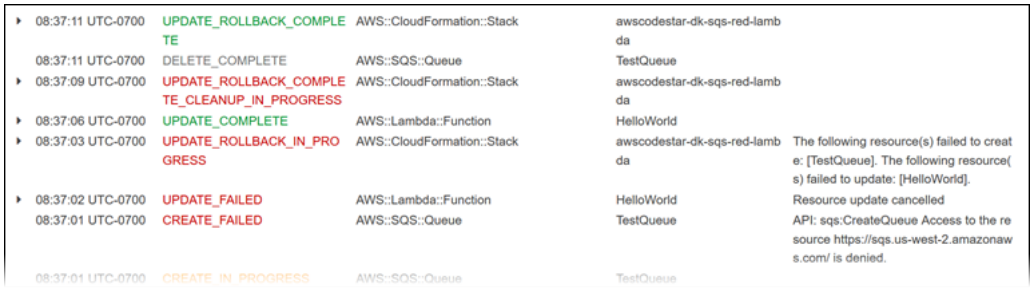
ステップ 4: AWS CloudFormation スタック更新をモニタリングする

1. プロジェクトのパイプラインがデプロイステージを開始すると、 AWS CloudFormation スタックの更新が開始されます。 AWS CodeStar ダッシュボードでパイプラインの AWS CloudFormation ステージを選択すると、スタックの更新を確認できます。

   トラブルシューティング：

   必要なリソースのアクセス許可が不足している場合、このスタック更新は失敗します。プロジェクトのパイプラインの AWS CodeStar ダッシュボードビューで障害ステータスを表示します。

   パイプラインのデプロイステージで CloudFormation リンクを選択して、 AWS CloudFormation コンソールで障害をトラブルシューティングします。コンソールの [Events] (イベント) リストで、プロジェクトを選択して、スタック作成の詳細を表示します。障害の詳細が記載されたメッセージが表示されます。この例では、`sqs:CreateQueue` のアクセス許可が不足しています。



   プロジェクトの AWS CloudFormation ワーカーロールにアタッチされたポリシーを編集して、不足しているアクセス許可を追加します。「ステップ 1: IAM で CloudFormation ワーカーロールを編集する」を参照してください。

2. パイプラインが正常に実行されると、 AWS CloudFormation スタックでリソースが作成されます。のリソースリストで AWS CloudFormation、プロジェクト用に作成されたリソースを表示します。この例では、TestQueue キューが [Resources] (リソース) セクションに一覧表示されています。

   キュー URL は で使用できます AWS CloudFormation。キュー URL はこの形式に従います。

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

   詳細については、[Send an Amazon SQS Message] (Amazon SQS メッセージの送信)、[Receive a Message from an Amazon SQS Queue] (Amazon SQS キューからのメッセージの受信)、および [Delete a Message from an Amazon SQS Queue] (Amazon SQS キューからのメッセージの削除) を参照してください。

ステップ 5: インラインポリシーでリソースのアクセス許可を追加する

新しいリソースへのアクセス権をチームメンバーに付与するには、適切なインラインポリシーをユーザーのロールに追加します。必ずしもすべてのリソースでアクセス許可を追加する必要があるわけではありません。以下のステップを実行するには、ルートユーザー、アカウントの管理者ユーザー、または AdministratorAccess 管理ポリシーか同等のポリシーが添付されている IAM ユーザーかフェデレーティッドユーザーとして、コンソールにサインイン済みである必要があります。

JSON ポリシーエディタでポリシーを作成するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/iam/:// www.com」で IAM コンソールを開きます。
2. 左側のナビゲーションペインで、[ポリシー] を選択します。

   初めて [ポリシー] を選択する場合には、[管理ポリシーにようこそ] ページが表示されます。[今すぐ始める] を選択します。
3. ページの上部で、[ポリシーを作成] を選択します。
4. [ポリシーエディタ] セクションで、[JSON] オプションを選択します。
5. 次の JSON ポリシードキュメントを入力します。

   ```
   {
    "Action": [
      "sqs:CreateQueue",
   ```

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

6. [次へ] をクリックします。

> **Note**
>
> いつでも [Visual] と [JSON] エディタオプションを切り替えることができます。ただし、[Visual] エディタで [次へ] に変更または選択した場合、IAM はポリシーを再構成して visual エディタに合わせて最適化することがあります。詳細については、「IAM ユーザーガイド」の「ポリシーの再構成」を参照してください。

7. [確認と作成] ページで、作成するポリシーの [ポリシー名] と [説明] (オプション) を入力します。[このポリシーで定義されているアクセス許可] を確認して、ポリシーによって付与されたアクセス許可を確認します。
8. [ポリシーの作成] をクリックして、新しいポリシーを保存します。

IAM ロールをプロジェクトに追加する

2018 年 12 月 6 日 (PDT) 時点では、アプリケーションスタック (template.yml) で独自のロールとポリシーを定義できます。特権のエスカレーションと破壊的なアクションのリスクを軽減するために、作成する IAM エンティティごとに、プロジェクト固有のアクセス許可の境界を設定する必要があります。複数の関数を含む Lambda プロジェクトがある場合は、関数ごとに IAM ロールを作成するのがベストプラクティスです。

IAM ロールをプロジェクトに追加するには

1. プロジェクトの `template.yml` ファイルを編集します。
2. `Resources:` セクションで、次の例の形式を使用して IAM リソースを追加します：

```
  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. パイプラインを通して変更をリリースし、成功を確認します。

Prod ステージとエンドポイントをプロジェクトに追加する

このセクションの手順を使用して、新しい本番稼働 (Prod) ステージをパイプラインに追加し、パイプラインの Deploy および Prod ステージ間に手動の承認ステージを追加します。これにより、プロジェクトのパイプラインが実行されるときに、追加のリソーススタックが作成されます。

> **Note**
>
> 次の場合は、以下の手順を使用できます：
>
> - 2018 年 8 月 3 日以降に作成されたプロジェクトの場合、 は Amazon EC2、Elastic Beanstalk、または Lambda プロジェクトをプロジェクトリポジトリに `/template.yml` ファイルで AWS CodeStar プロビジョニングしました。
> - 2018 年 12 月 6 日以降に作成されたプロジェクトの場合、 はアクセス許可の境界ポリシーを使用してプロジェクトを AWS CodeStar プロビジョニングしました。

すべての AWS CodeStar プロジェクトは、Linux AWS インスタンスや Lambda 関数など、アプリケーションのランタイム依存関係をモデル化する CloudFormation テンプレートファイルを使用します。この `/template.yml` ファイルは、ソースリポジトリに保存されています。

/template.yml ファイルで、Stage パラメータを使用して、プロジェクトパイプラインの新しいステージのリソーススタックを追加します。

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

Stage パラメータは、リソースでプロジェクト ID が参照されているすべての名前付きリソースに適用されます。たとえば、次のロール名は、テンプレート内の名前付きリソースです：

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

前提条件

AWS CodeStar コンソールのテンプレートオプションを使用してプロジェクトを作成します。

IAM ユーザーに次のアクセス許可があることを確認します：

- iam:PassRole プロジェクト CloudFormation ロールの 。
- プロジェクトツールチェーンロールの iam:PassRole。
- cloudformation:DescribeStacks
- cloudformation:ListChangeSets

Elastic Beanstalk または Amazon EC2 プロジェクトの場合のみ:

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

トピック

- ステップ 1: CodeDeploy で新しいデプロイグループを作成する (Amazon EC2 プロジェクトのみ)
- ステップ 2: Prod ステージの新しいパイプラインステージを追加する
- ステップ 3: 手動承認ステージを追加する
- ステップ 4: AWS CloudFormation 変更をプッシュし、スタックの更新をモニタリングする

ステップ 1: CodeDeploy で新しいデプロイグループを作成する (Amazon EC2 プロジェクトのみ)

CodeDeploy アプリケーションを選択し、新しいインスタンスに関連付けられた新しいデプロイグループを追加します。

> **Note**
>
> プロジェクトが Lambda または Elastic Beanstalk プロジェクトである場合は、このステップはスキップできます。

1. https://console.aws.amazon.com/codedeploy で、CodeDeploy コンソールを開きます。
2. AWS CodeStarで作成されたときにプロジェクト用に生成された CodeDeploy アプリケーションを選択します。
3. [Deployment groups] (デプロイグループ) で、[Create deployment group] (デプロイグループの作成) を選択します。
4. [Deployment group name] (デプロイグループ名) に「***<project-id>-prod-Env***」と入力します。
5. サービスロールで、 AWS CodeStar プロジェクトのツールチェーンワーカーロールを選択します。
6. [Deployment type] (デプロイタイプ) で、[In-place] (インプレース) を選択します。
7. [Environment configuration] (環境設定) で、[Amazon EC2 Instances] (Amazon EC2 インスタンス) タブを選択します。
8. [Tag](タグ)グループで、[Key] (キー) の [`aws:cloudformation:stack-name`] を選択します。[Value] (値) で、[`awscodestar-<projectid>-infrastructure-prod`] (GenerateChangeSet アクション用に作成されるスタック) を選択します。
9. [Deployment settings] (デプロイ設定) で [`CodeDeployDefault.AllAtOnce`] を選択します。
10. [Choose a load balancer] (ロードバランサーを選択) をクリアします。

11. [Create deployment group] (デプロイグループの作成) を選択します。

    これで、2 番目のデプロイグループが作成されました。

ステップ 2: Prod ステージの新しいパイプラインステージを追加する

プロジェクトの Deploy ステージと同じ一連のデプロイアクションを使用してステージを追加します。たとえば、Amazon EC2 プロジェクトの新しい Prod ステージには、プロジェクト用に作成された [Deploy] (デプロイ) ステージと同じアクションが必要です。

[Deploy] (デプロイ) ステージからパラメータおよびフィールドをコピーするには

1. AWS CodeStar プロジェクトダッシュボードから、パイプラインの詳細を選択して、CodePipeline コンソールでパイプラインを開きます。
2. [編集] を選択します。
3. [Deploy] (デプロイ) ステージで、[Edit stage] (ステージを編集) を選択します。
4. [GenerateChangeSet] アクションの編集アイコンを選択します。次のフィールドの値を書き留めておきます。下記の値は、新しいアクションの作成時に使用します。

   - スタックの名前
   - 変更セット名
   - テンプレート
   - テンプレート構成
   - 入力アーティファクト
5. [Advanced] (詳細) を展開し、[Parameters] (パラメータ) で、プロジェクトのパラメータをコピーします。これらのパラメータを新しいアクションに貼り付けます。例えば、ここに表示されるパラメータを JSON 形式でコピーします。

   - Lambda プロジェクト:

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

   - Amazon EC2 プロジェクト:

     ```
     {
     ```

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

- Elastic Beanstalk プロジェクト：

```
{
  "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. ステージの編集ペインで、[Cancel] (キャンセル) を選択します。

新しい Prod ステージで GenerateChangeSet アクションを作成するには

> **Note**
>
> 新しいアクションを追加した後編集モードのまま、編集のために新しいアクションを再度開くと、一部のフィールドが表示されない場合があります。また、以下が表示される場合があります：スタック stack-name は存在しません
> このエラーが出てもパイプラインを保存することはできます。ただし、表示されないフィールドを復元するには、新しいアクションを削除してから再び追加する必要があります。パイプラインを保存して実行した後、スタックが認識されエラーが表示されなくなります。

1. パイプラインがまだ表示されていない場合は、 AWS CodeStar プロジェクトダッシュボードからパイプラインの詳細を選択して、コンソールでパイプラインを開きます。
2. [編集] を選択します。

3. 図の最下部で [+ Add stage] (+ ステージの追加) を選択します。
4. ステージ名 (例：**Prod**) を入力し、[+ Add action group] (+ アクショングループの追加) を選択します。
5. [Action name] (アクション名) に、名前を入力します (例：**GenerateChangeSet**)。
6. [Action provider] (アクションプロバイダ) で、[AWS CloudFormation] を選択します。
7. [Action mode] (アクションモード) で [Create or replace a change set] (変更セットの作成または置換) を選択します。
8. スタック名に、このアクションによって作成される CloudFormation スタックの新しい名前を入力します。デプロイスタック名と同じ名前でスタートし、**-prod** を追加します:

   - Lambda プロジェクト:`awscodestar-<project_name>-lambda-prod`
   - Amazon EC2 および Elastic Beanstalk プロジェクト:`awscodestar-<project_name>-infrastructure-prod`

   > **Note**
   >
   > スタックは正確に **awscodestar-<project_name>-** で始まる必要があり、それ以外の場合はスタックの作成は失敗します。

9. [Change set name] (変更セット名) で、既存の [Deploy] (デプロイ) ステージ (例：**pipeline-changeset**) で指定されたのと同じ変更セット名を入力します。
10. [Input artifacts] (入力アーティファクト) で、[Build artifact] (ビルドアーティファクト) を選択します。
11. [Template] (テンプレート) で、既存の [Deploy] (デプロイ) ステージ (例：**<project-ID>-BuildArtifact::template.yml**) で指定されたのと同じ変更テンプレート名を入力します。
12. [Template configuration] (テンプレート設定) で、デプロイステージ (例：**<project-ID>-BuildArtifact::template-configuration.json**) で指定されたのと同じ変更テンプレート設定ファイル名を入力します。
13. [Capabilities] (機能) で、 CAPABILITY_NAMED_IAM を選択します。
14. [Role name](ロール名) で、プロジェクトの CloudFormation ワーカーロールの名前を選択します。
15. [Advanced] (詳細) を展開し、[Parameters] (パラメータ) で、プロジェクトのパラメータを貼り付けます。Amazon EC2 プロジェクト用に、ここに示すように JSON 形式で`Stage` パラメータを含めます：

```
{

  "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**
>
> 変更するパラメータだけではなく、プロジェクトのすべてのパラメータを貼り付けます。

16. [Save] を選択します。
17. AWS CodePipeline ペインで、パイプラインの変更を保存 を選択し、変更を保存 を選択します。

> **Note**
>
> 変更検出リソースの削除および追加を通知するメッセージが表示されることがあります。メッセージを確認して、このチュートリアルの次のステップに進みます。

更新されたパイプラインを表示します。

新しい Prod ステージで ExecuteChangeSet アクションを作成するには

1. パイプラインをまだ表示していない場合は、 AWS CodeStar プロジェクトダッシュボードからパイプラインの詳細を選択して、コンソールでパイプラインを開きます。
2. [編集] を選択します。
3. 新しい Prod ステージで、新しい GenerateChangeSet アクションの後で、[+ Add action group] (+ アクショングループの追加) を選択します。

4. [Action name] (アクション名) に、名前を入力します (例：**ExecuteChangeSet**)。
5. [Action provider] (アクションプロバイダ) で、[AWS CloudFormation] を選択します。
6. [Action mode] (アクションモード) で、 [Execute a change set] (変更セットの実行) を選択します。
7. スタック名に、GenerateChangeSet アクションに入力した CloudFormation スタックの新しい名前を入力します (例: **awscodestar-<project-ID>-infrastructure-prod**)。
8. [Change set name] (変更セット名) で、[Deploy] (デプロイ) ステージで使用したのと同じ変更セット名 (例：**pipeline-changeset**) を入力します。
9. [Done] (完了) を選択します。
10. AWS CodePipeline ペインで、パイプラインの変更を保存を選択し、変更を保存を選択します。

> **Note**
>
> 変更検出リソースの削除および追加を通知するメッセージが表示されることがあります。メッセージを確認して、このチュートリアルの次のステップに進みます。

更新されたパイプラインを表示します。

新しい Prod ステージで CodeDeploy デプロイアクションを作成するには (Amazon EC2 プロジェクトのみ)

1. Prod ステージの新しいアクションの後、[+ Action] (+ アクション) を選択します。
2. [Action name] (アクション名) に、名前を入力します (例：**Deploy**)。
3. [Action provider] (アクションプロバイダ) で、[AWS CodeDeploy] を選択します。
4. [Application name] (アプリケーション名) で、プロジェクトの CodeDeploy アプリケーションの名前を選択します。
5. [Deployment group] (デプロイグループ) で、ステップ 2 で作成した新しい CodeDeploy デプロイグループの名前を選択します。
6. [Input artifacts] (入力アーティファクト) で、既存のステージで使用されたのと同じビルドアーティファクトを選択します。
7. [Done] (完了) を選択します。
8. AWS CodePipeline ペインで、パイプラインの変更を保存を選択し、変更を保存を選択します。更新されたパイプラインを表示します。

ステップ 3: 手動承認ステージを追加する

ベストプラクティスとして、新しい本番稼働ステージの前に手動承認ステージを追加します。

1. 左上の [Edit] (編集) を選択します。
2. パイプラインの図で、[Deploy] (デプロイ) と [Prod deployment] (Prod デプロイ)ステージの間で、[+ Add stage] (+ ステージの追加) を選択します。
3. [Edit stage] (ステージを編集) で、ステージ名 (例：**Approval**) を入力し、[+ Add action group] (+ アクショングループの追加) を選択します。
4. [Action name] (アクション名) に、名前を入力します (例：**Approval**)。
5. [Approval type] (承認の種類) で、[Manual approval] (手動承認) を選択します。
6. (オプション) [Configuration] (設定) の [SNS Topic ARN] (SNS トピック ARN) で、作成してサブスクライブした SNS トピックを選択します。
7. [Add Action] (アクションの追加) を選択します。
8. AWS CodePipeline ペインで、パイプラインの変更を保存を選択し、変更を保存を選択します。更新されたパイプラインを表示します。
9. 変更を送信してパイプラインの構築をスタートするには、[Release change] (変更のリリース)、[Release] (リリース) の順に選択します。

ステップ 4: AWS CloudFormation 変更をプッシュし、スタックの更新をモニタリングする

1. パイプラインの実行中に、次の手順を使用して、新しいステージのスタックとエンドポイントの作成をフォローすることができます。
2. パイプラインがデプロイステージを開始すると、 AWS CloudFormation スタックの更新が開始されます。 AWS CodeStar ダッシュボードでパイプラインの AWS CloudFormation ステージを選択すると、スタックの更新通知を表示できます。スタック作成の詳細を表示するには、コンソールで、[Events] (イベント) リストからプロジェクトを選択します。
3. パイプラインが正常に完了すると、リソースが AWS CloudFormation スタックに作成されます。 AWS CloudFormation コンソールで、プロジェクトのインフラストラクチャスタックを選択します。スタック名は次の形式に従います：

   - Lambda プロジェクト:`awscodestar-<project_name>-lambda-prod`
   - Amazon EC2 および Elastic Beanstalk プロジェクト:`awscodestar-<project_name>-infrastructure-prod`

AWS CloudFormation コンソールのリソースリストで、プロジェクト用に作成されたリソースを表示します。この例では、新しい Amazon EC2 インスタンスが [Resources] (リソース) セクションに表示されます。

4. 本番稼働ステージのエンドポイントにアクセスします：

   - Elastic Beanstalk プロジェクトの場合は、 AWS CloudFormation コンソールで新しいスタックを開き、リソースを展開します。Elastic Beanstalk アプリケーションを選択します。Elastic Beanstalk コンソールでリンクが開きます。[Environments] (環境) を選択します。[URL] で URL を選択し、ブラウザでエンドポイントを開きます。
   - Lambda プロジェクトの場合は、 AWS CloudFormation コンソールで新しいスタックを開き、リソースを展開します。[API Gateway resource](API Gateway リソース) を選択します。リンクが API Gateway コンソールで開きます。[Stages] (ステージ) を選択します。[Invoke URL] (呼び出し URL) で URL を選択し、ブラウザでエンドポイントを開きます。
   - Amazon EC2 プロジェクトの場合は、 AWS CodeStar コンソールのプロジェクトリソースリストで新しい Amazon EC2 インスタンスを選択します。Amazon EC2 コンソールの[Instance] (インスタンス) ページでリンクが開きます。[Description] (説明) タブを選択し、[Public DNS (IPv4)] (パブリック DNS (IPv4)) の URL をコピーして、ブラウザでその URL を開きます。

5. 変更がデプロイされていることを確認します。

AWS CodeStar プロジェクトで SSM パラメータを安全に使用する

多くのお客様は認証情報などの機密情報を [Systems Manager Parameter Store] (システムマネージャパラメータストア) のパラメータに保存します。 AWS CodeStar プロジェクトでこれらのパラメータを安全に使用できるようになりました。例えば、CodeBuild のビルド仕様や、ツールチェーンスタック (template.yml) でアプリケーションリソースを定義する際に、SSM パラメータを使用する場合です。

AWS CodeStar プロジェクトで SSM パラメータを使用するには、AWS CodeStar プロジェクト ARN を使用してパラメータに手動でタグ付けする必要があります。 また、タグ付けしたパラメータにアクセスするための適切なアクセス許可を AWS CodeStar ツールチェーンのワーカーロールに指定する必要もあります。

開始する前に

- [Create a new] (新規作成) または、アクセスする情報を含む既存の Systems Manager パラメータを特定します。

- 使用する AWS CodeStar プロジェクトを特定するか、[create a new project] (新しいプロジェクトを作成) します。
- CodeStar プロジェクトの ARN を書き留めます。以下のような形式です：`arn:aws:codestar:region-id:account-id:project/project-id`

AWS CodeStar プロジェクトの ARN を使用してパラメータにタグ付けします。

ステップバイステップの手順については、[Tagging Systems Manager Parameters] (システムマネージャパラメータへのタグ付け) を参照してください。

1. [Key] (キー) に、「`awscodestar:projectArn`」と入力します。
2. [Value] (値) には、CodeStar のプロジェクト ARN (`arn:aws:codestar:region-id:account-id:project/project-id`) を入力します。
3. [Save] (保存) を選択します。

これで、template.yml ファイルで SSM パラメータをリファレンスできるようになります。ツールチェーンのワーカーロールで使用する場合は、追加のアクセス許可を付与する必要があります。

AWS CodeStar プロジェクトのツールチェーンでタグ付けされたパラメータを使用するためにアクセス許可を付与する

> **Note**
>
> 以下のステップは、2018 年 12 月 6 日 (PDT) 以降に作成されたプロジェクトにのみ適用されます。

1. 使用するプロジェクトの AWS CodeStar プロジェクトダッシュボードを開きます。
2. [Project] (プロジェクト) をクリックして作成済みリソースのリストを表示し、ツールチェーンのワーカーロールを見つけます。`role/CodeStarWorker-project-id-ToolChain` という形式の名前の IAM リソースです。
3. ARN をクリックして、IAM コンソールで開きます。
4. ToolChainWorkerPolicy を見つけ、必要に応じて展開します。
5. [Edit Policy] (ポリシーの編集) をクリックします。
6. `Action:` の下に次の行を追加します：

```
ssm:GetParameter*
```

7. [Review policy] (ポリシーの確認) をクリックしてから、[Save changes] (変更の保存) をクリックします。

2018 年 12 月 6 日 (PDT) 以前に作成されたプロジェクトの場合は、次のアクセス許可を各サービスのワーカーロールに追加する必要があります。

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

AWS Lambda プロジェクトのトラフィックを移行する

AWS CodeDeploy は、サーバーレスプロジェクトの関数の AWS Lambda 関数 AWS CodeStar バージョンデプロイをサポートします。 AWS Lambda デプロイは、受信トラフィックを既存の Lambda 関数から更新された Lambda 関数バージョンに移行します。更新された Lambda 関数をテストするには、別のバージョンをデプロイし、必要に応じて、デプロイを最初のバージョンにロールバックします。

このセクションのステップを使用して、 AWS CodeStar プロジェクトテンプレートを変更し、CodeStarWorker ロールの IAM アクセス許可を更新します。このタスクは、エイリアスされた AWS Lambda 関数を作成する で AWS CloudFormation 自動レスポンスを開始し、更新された環境にトラフィックをシフト AWS CodeDeploy するように に指示します。

> **Note**
>
> 2018 年 12 月 12 日以前に AWS CodeStar プロジェクトを作成した場合にのみ、これらのステップを完了します。

AWS CodeDeploy には、アプリケーションの AWS Lambda 関数のバージョンにトラフィックを移行できる 3 つのデプロイオプションがあります。

- Canary: トラフィックは 2 つの増分で移行されます。残りのトラフィックが 2 回目の増分で移行される前に、最初の増分および間隔で更新された Lambda 関数のバージョンに移行されるトラフィックの割合 (%) を分単位で指定する、事前定義された Canary オプションから選択できます。
- Linear: トラフィックは等しい増分で移行され、増分間の間隔 (分) も同じです。増分ごとに移行するトラフィックの割合 (%) と、増分間の間隔 (分) を指定する、事前定義済み線形オプションから選択できます。トラフィックは毎回同じ間隔 (分) の等しい増分で移行されます。増分ごとに移行するトラフィックの割合 (%) と、増分間の間隔 (分) を指定する、事前定義済み線形オプションから選択できます。
- All-at-once: すべてのトラフィックは元の Lambda 関数から最新バージョンの Lambda 関数に一度に移行されます。

デプロイプリファレンスのタイプ
Canary10Percent30Minutes
Canary10Percent5Minutes
Canary10Percent10Minutes
Canary10Percent15Minutes
Linear10PercentEvery10Minutes
Linear10PercentEvery1Minute
Linear10PercentEvery2Minutes
Linear10PercentEvery3Minutes

デプロイプリファレンスのタイプ
AllAtOnce

AWS Lambda コンピューティングプラットフォームでの AWS CodeDeploy デプロイの詳細については、AWS 「Lambda コンピューティングプラットフォームでのデプロイ」を参照してください。

SAM の詳細については、GitHub AWS のAWS 「サーバーレスアプリケーションモデル (AWS SAM)」を参照してください。

前提条件:

サーバーレスプロジェクトを作成する場合、Lambda コンピューティングプラットフォームで任意のテンプレートを選択します。ステップ 4 ~ 6 を実行するには、管理者ユーザーとしてサインインする必要があります。

ステップ 1: SAM テンプレートを変更して AWS Lambda バージョンデプロイパラメータを追加する

1. AWS CodeStar コンソールを https://console.aws.amazon.com/codestar/://www.com で開きます。
2. プロジェクトを作成するか、`template.yml` ファイルを含む既存のプロジェクトを選択して、[Code] (コード) ページを開きます。リポジトリの最上位で、変更する `template.yml` という名前の SAM テンプレートの場所を書き留めます。
3. `template.yml` ファイルを IDE またはローカルリポジトリで開きます。以下のテキストをコピーして、`Globals` セクションをファイルに追加します。このチュートリアルのサンプルテキストでは、`Canary10Percent5Minutes` オプションを選択します。

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

この例では、`Globals` セクション追加後に変更されたテンプレートを示します。

```
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:
```

詳細については、SAM テンプレートの グローバルセクション リファレンスガイドを参照してください。

ステップ 2: CloudFormation ロールを編集してアクセス許可を追加する

1. にサインイン AWS マネジメントコンソール し、 AWS CodeStar コンソールを https://console.aws.amazon.com/codestar/://www.com で開きます。

   > **Note**
   >
   > で作成または識別した IAM ユーザーに関連付けられた認証情報 AWS マネジメントコンソール を使用して にサインインする必要がありますAWS CodeStarのセットアップ。このユーザーには、 という AWS 名前の管理ポリシーが**AWSCodeStarFullAccess**アタッチされている必要があります。

2. 既存のサーバーレスプロジェクトを選択し、[Project resources] (プロジェクトリソース) ページを開きます。
3. リソースで、CodeStarWorker/AWS CloudFormation role 用に作成された IAM ロールを選択します。ロールが IAM コンソールで開きます。
4. [Permissions] (アクセス許可) タブの [Inline Policies] (インラインポリシー) で、サービスロールポリシーの列の [Edit Policy] (ポリシーの編集) を選択します。[JSON] タブを選択して、JSON 形式でポリシーを編集します。

> **Note**
>
> サービスロールは CodeStarWorkerCloudFormationRolePolicy という名前になります。

5. [JSON] フィールドで、Statement 要素内に次のポリシーステートメントを追加します。*region* と *id* のプレースホルダーは、お客様のリージョンとアカウント ID に置き換えてください。

```
{
  "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. [Review policy] (ポリシーの確認) を選択して、ポリシーにエラーがないことを確認します。ポリシーにエラーがなければ、[Save changes] (変更の保存) を選択します。

ステップ 3: テンプレートの変更をコミットしてプッシュし、 AWS Lambda バージョンシフトを開始する

1. ステップ 1 で保存した `template.yml` ファイルの変更をコミットおよびプッシュします。

> **Note**
>
> これにより、パイプラインが開始されます。IAM アクセス許可を更新する前に変更をコミットすると、パイプラインが起動し、 AWS CloudFormation スタックの更新がロールバックするエラーが発生します。この問題が発生した場合は、アクセス許可を修正してから、パイプランを再起動します。

2. AWS CloudFormation スタックの更新は、プロジェクトのパイプラインがデプロイステージを開始すると開始されます。デプロイの開始時にスタックの更新通知を表示するには、 AWS CodeStar ダッシュボードでパイプラインの AWS CloudFormation ステージを選択します。

   スタックの更新中に、 は次のようにプロジェクトリソース AWS CloudFormation を自動的に更新します。

   - AWS CloudFormation は、エイリアス化された Lambda 関数、イベントフック、リソースを作成して`template.yml`ファイルを処理します。
   - AWS CloudFormation は Lambda を呼び出して、関数の新しいバージョンを作成します。
   - AWS CloudFormation は AppSpec ファイルを作成し、 を呼び出し AWS CodeDeploy てトラフィックをシフトします。

   SAM でのエイリアスの Lambda 関数の発行の詳細については、AWS サーバーレスアプリケーションモデル(SAM) テンプレートリファレンスを参照してください。 AWS CodeDeploy AppSpec ファイル内のイベントフックとリソースの詳細については、「Lambda デプロイの AppSpec 'resources' セクション (AWS Lambda デプロイのみ) 」およびAppSpec 'hooks' セクション AWS」を参照してください。

3. パイプラインが正常に完了すると、 AWS CloudFormation スタックでリソースが作成されます。プロジェクトページのプロジェクトリソースリストで、プロジェクト用に作成された AWS CodeDeploy アプリケーション、 AWS CodeDeploy デプロイグループ、および AWS CodeDeploy サービスロールリソースを表示します。

4. 新しいバージョンを作成するには、リポジトリで Lambda 関数を変更します。新しいデプロイが開始し、トラフィックは、SAM テンプレートで示されるデプロイタイプに応じて、移行されます。新しいバージョンに移行されるトラフィックのステータスを表示するには、[Project] (プロジェクト) ページの [Project Resources] (プロジェクトリソース) リストで、AWS CodeDeploy デプロイへのリンクを選択します。

5. 各リビジョンの詳細を表示するには、リビジョンで、 AWS CodeDeploy デプロイグループへのリンクを選択します。

6. ローカル作業ディレクトリでは、 AWS Lambda 関数を変更し、プロジェクトリポジトリに変更をコミットできます。 AWS CodeDeploy AWS CloudFormation は、同じ方法で次のリビジョンを管理できます。Lambda デプロイの再デプロイ、停止、またはロールバックの詳細については、AWS 「Lambda コンピューティングプラットフォームでのデプロイ」を参照してください。

AWS CodeStar プロジェクトを本番稼働用に移行する

AWS CodeStar プロジェクトを使用してアプリケーションを作成し、AWS CodeStar が提供する内容を確認したら、プロジェクトを本番稼働に移行することができます。これを行う 1 つの方法は、アプリケーションの AWS リソースを AWS CodeStar の外部にレプリケートすることです。リポジトリ、ビルドプロジェクト、パイプライン、デプロイは引き続き必要ですが、それらを AWS CodeStar で作成するのではなく、 CloudFormationを使用して再作成します。

> **Note**
>
> 最初に AWS CodeStar クイックスタートの 1 つを使用して類似したプロジェクトを作成または表示し、それを独自のプロジェクトのテンプレートとして使用して、必要なリソースとポリシーを確実に含めるようにすると便利です。

AWS CodeStar プロジェクトは、コードをデプロイするために作成されたソースコードとリソースの組み合わせです。コードのビルド、リリース、デプロイに役立つリソースのコレクションは、ツールチェーンリソースと呼ばれます。プロジェクトの作成時に、 CloudFormation テンプレートはツールチェーンリソースを継続的インテグレーション/継続的デプロイ (CI/CD) パイプラインにプロビジョニングします。

コンソールでプロジェクトを作成すると、ツールチェーンテンプレートが作成されます。を使用してプロジェクト AWS CLI を作成する場合は、ツールチェーンリソースを作成するツールチェーンテンプレートを作成します。

完全なツールチェーンを作成するには、次の推奨リソースが必要です：

1. ソースコードを保存する CodeCommit または GitHub リポジトリ。
2. リポジトリへの変更をリッスンするよう設定されている CodePipeline パイプライン。
   a. AWS CodeBuild を使用してユニットテストまたは統合テストを使用する場合は、ビルドステージをパイプラインに追加してビルドアーティファクトを作成することをお勧めします。
   b. CodeDeploy または を使用してビルドアーティファクトとソースコードをランタイムインフラストラクチャ CloudFormation にデプロイするデプロイステージをパイプラインに追加することをお勧めします。

> **Note**
>
> CodePipeline では、2 つ以上のステージがパイプラインに必要であり、最初のステージはソースステージにする必要があるため、ビルドステージまたはデプロイステージを 2 番目のステージとして追加します。

トピック

GitHub リポジトリを作成する

ツールチェーンテンプレートで定義して、GitHub リポジトリを作成します。コードをリポジトリにアップロードできるように、ソースコードを含む ZIP ファイルの場所がすでに作成されていることを確認します。また、 がユーザーに代わって GitHub AWS に接続できるように、GitHub で個人用アクセストークンを作成しておく必要があります。GitHub の個人用アクセストークンに加えて、渡す Code オブジェクトに対する `s3.GetObject` アクセス許可も必要です。

パブリック GitHub リポジトリを指定するには、 CloudFormationのツールチェーンテンプレートに次のようなコードを追加します。

```
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
```

このコードは次の情報を指定します。

- 組み込みたいコードの場所、Amazon S3 バケットである必要があります。
- GitHub リポジトリで課題を有効にするかどうか。
- GitHub リポジトリがプライベートであるかどうか。
- 作成した GitHub 個人用アクセストークン。
- 作成するリポジトリの説明、名前、所有者。

指定する情報の詳細については、AWS CloudFormation ユーザーガイドの AWS::CodeStar::GitHubRepository を参照してください。

でのプロジェクトタグの使用 AWS CodeStar

AWS CodeStarでタグをプロジェクトに関連付けることができます。タグは、プロジェクトを管理するのに役立ちます。例えば、ベータ版リリースで組織が進めているプロジェクトに `Release` キーと `Beta` の値を持つタグを追加できます。

プロジェクトにタグを追加する

1. AWS CodeStar コンソールでプロジェクトを開き、サイドナビゲーションペインで設定を選択します。
2. [Tags] (タグ) で、[Edit] (編集) を選択します。
3. [Key] (キー) に、タグの名前を入力します。[Value] (値) に、タグの値を入力します。
4. オプション：[Add tag] (タグの追加) を選択して、複数のタグを追加します。
5. タグの追加が終了したら、[Save] (保存) を選択します。

プロジェクトからタグを削除する

1. AWS CodeStar コンソールでプロジェクトを開き、サイドナビゲーションペインで設定を選択します。
2. [Tags] (タグ) で、[Edit] (編集) を選択します。
3. [Tags] (タグ) で、削除するタグを見つけ、[Remove tag] (タグの削除) を選択します。
4. [Save] (保存) を選択します。

プロジェクトのタグのリストを取得します。

を使用して コマンド AWS CLI AWS CodeStar list-tags-for-projectを実行し、プロジェクトの名前を指定します。

```
aws codestar list-tags-for-project --id my-first-projec
```

成功すると、次のようなタグのリストが出力に表示されます。

```
{
  "tags": {
    "Release": "Beta"
  }
}
```

AWS CodeStar プロジェクトの削除

プロジェクトが不要になった場合は、プロジェクトとそのリソースを削除して、 AWSで追加料金が発生しないようにします。プロジェクトを削除すると、すべてのチームメンバーはそのプロジェクトから削除されます。プロジェクトロールは IAM ユーザーから削除されますが、 のユーザープロファイル AWS CodeStar は変更されません。 AWS CodeStar コンソールまたは を使用してプロジェクト AWS CLI を削除できます。プロジェクトを削除するには、 AWS CodeStar サービスロール が必要です。これは変更されず`aws-codestar-service-role`、 によって引き受け可能である必要があります AWS CodeStar。

> **Important**
>
> でのプロジェクトの削除は元に戻す AWS CodeStar ことができません。デフォルトでは、プロジェクトのすべての AWS リソースは、以下を含む AWS アカウントで削除されます。
>
> - プロジェクトの CodeCommit リポジトリと、そのリポジトリに保存されているすべてのもの。
> - AWS CodeStar プロジェクトロール、およびプロジェクトとそのリソース用に設定された関連する IAM ポリシー。
> - プロジェクト用に作成されたすべての Amazon EC2 インスタンス。
> - 次のような、デプロイアプリケーションと関連リソース。
>   - CodeDeploy アプリケーションおよび関連するデプロイグループ。

- AWS Lambda 関数および関連する API Gateway APIs。
- AWS Elastic Beanstalk アプリケーションおよび関連する環境。

- CodePipeline でのプロジェクトの継続的なデプロイパイプライン。
- プロジェクトに関連付けられた AWS CloudFormation スタック。
- AWS CodeStar コンソールで作成された AWS Cloud9 開発環境。この環境でコミットされていないコードの変更はすべて、失われます。

プロジェクトと一緒に、プロジェクトリソースをすべて削除するには、[Delete resources] (リソースを削除) チェックボックスをオンにします。このオプションをオフにすると、プロジェクトは で削除され AWS CodeStar、それらのリソースへのアクセスを有効にしたプロジェクトロールは IAM で削除されますが、他のすべてのリソースは保持されます。では、これらのリソースに対して引き続き料金が発生する場合があります AWS。1 つ以上のリソースが不要になると判断した場合は、それらを手動で削除する必要があります。詳細については、「プロジェクトの削除: AWS CodeStar プロジェクトは削除されましたが、リソースはまだ存在します」を参照してください。
プロジェクトを削除する際にリソースを保持することにした場合は、ベストプラクティスとして、[Project details] (プロジェクトの詳細) ページからリソースのリストをコピーします。このように、プロジェクトがなくなっても、保有しているすべてのリソースのレコードは削除されません。

トピック

- AWS CodeStar のプロジェクトを削除する (コンソール)
- AWS CodeStar (AWS CLI) でプロジェクトを削除する

AWS CodeStar のプロジェクトを削除する (コンソール)

AWS CodeStar コンソールを使用してプロジェクトを削除できます。

でプロジェクトを削除するには AWS CodeStar

1. AWS CodeStar コンソールを https://console.aws.amazon.com/codestar/://https://https://https://https://https://https
2. ナビゲーションペインで、[Projects] (プロジェクト) を選択します。
3. 削除するプロジェクトを選択して、[Delete] (削除) を選択します。

または、プロジェクトを開き、コンソールの左側のナビゲーションペインから [Settings] (設定) を選択します。[Project details] (プロジェクトの詳細)ページで、[Delete project] (プロジェクトの削除) を選択します。

4. [Delete confirmation page] (削除の確認ページ) で、[delete] (削除) と入力します。プロジェクトリソースを削除する場合、[Delete resources] (リソースの削除) を選択したままにします。[Delete] (削除) を選択します。

   プロジェクトの削除には数分かかる場合があります。削除されると、プロジェクトは AWS CodeStar コンソールのプロジェクトのリストに表示されなくなります。

> **Important**
>
> プロジェクトで 以外のリソース AWS (GitHub リポジトリや Atlassian JIRA の問題など) を使用している場合、チェックボックスをオンにしても、それらのリソースは削除されません。
> IAM ユーザーではないロールに AWS CodeStar 管理ポリシーを手動でアタッチしている場合、プロジェクトを削除することはできません。プロジェクトの管理ポリシーをフェデレーティッドユーザーのロールに添付している場合は、プロジェクトを削除する前にポリシーをデタッチする必要があります。詳細については、「???」を参照してください。

AWS CodeStar （ AWS CLI) でプロジェクトを削除する

を使用してプロジェクト AWS CLI を削除できます。

でプロジェクトを削除するには AWS CodeStar

1. ターミナル (Linux、macOS、または Unix) またはコマンドプロンプト (Windows) で、プロジェクト名を含む delete-project コマンドを実行します。たとえば、ID *my-2nd-project* のプロジェクトを削除するには、次のように入力します：

```
aws codestar delete-project --id my-2nd-project
```

   このコマンドは、次のような出力を返します：

```
{
```

```
    "projectArn":"arn:aws:codestar:us-east-2:111111111111:project/my-2nd-project"
}
```

プロジェクトはすぐには削除されません。

2. プロジェクトの名前を含めて、describe-project コマンドを実行します。たとえば、ID が *my-2nd-project* のプロジェクトのステータスを確認するには、次のようなコマンドを実行します。

```
aws codestar describe-project --id my-2nd-project
```

プロジェクトがまだ削除されていない場合、このコマンドは以下のような出力を返します：

```
{
    "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"
    }
}
```

プロジェクトが削除されている場合、このコマンドは以下のような出力を返します：

```
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. list-projects コマンドを実行し、削除されたプロジェクトが AWS アカウントに関連付けられたプロジェクトのリストに表示されないことを確認します。

```
aws codestar list-projects
```

AWS CodeStar Teams の使用

開発プロジェクトを作成したら、一緒に作業できるように他のユーザーにアクセス権を付与します。では AWS CodeStar、各プロジェクトにプロジェクトチームがあります。ユーザーは複数の AWS CodeStar プロジェクトに属し、それぞれに異なる AWS CodeStar ロール (つまり、異なるアクセス許可) を持つことができます。 AWS CodeStar コンソールでは、ユーザーは AWS アカウントに関連付けられているすべてのプロジェクトを表示できますが、チームメンバーであるプロジェクトのみを表示して操作できます。

チームメンバーは自分のわかりやすい名前を選択できます。また、他のチームメンバーと連絡できるように E メールアドレスを追加できます。所有者でないチームメンバーがプロジェクトの AWS CodeStar ロールを変更することはできません。

の各プロジェクト AWS CodeStar には 3 つのロールがあります。

AWS CodeStar プロジェクトのロールとアクセス許可

ロール名	プロジェクトダッシュボードとステータスの表示	プロジェクトリソースの追加、削除、アクセス	チームメンバーの追加と削除	プロジェクトの削除
所有者	x	x	x	x
寄稿者	x	x		
閲覧者	x			

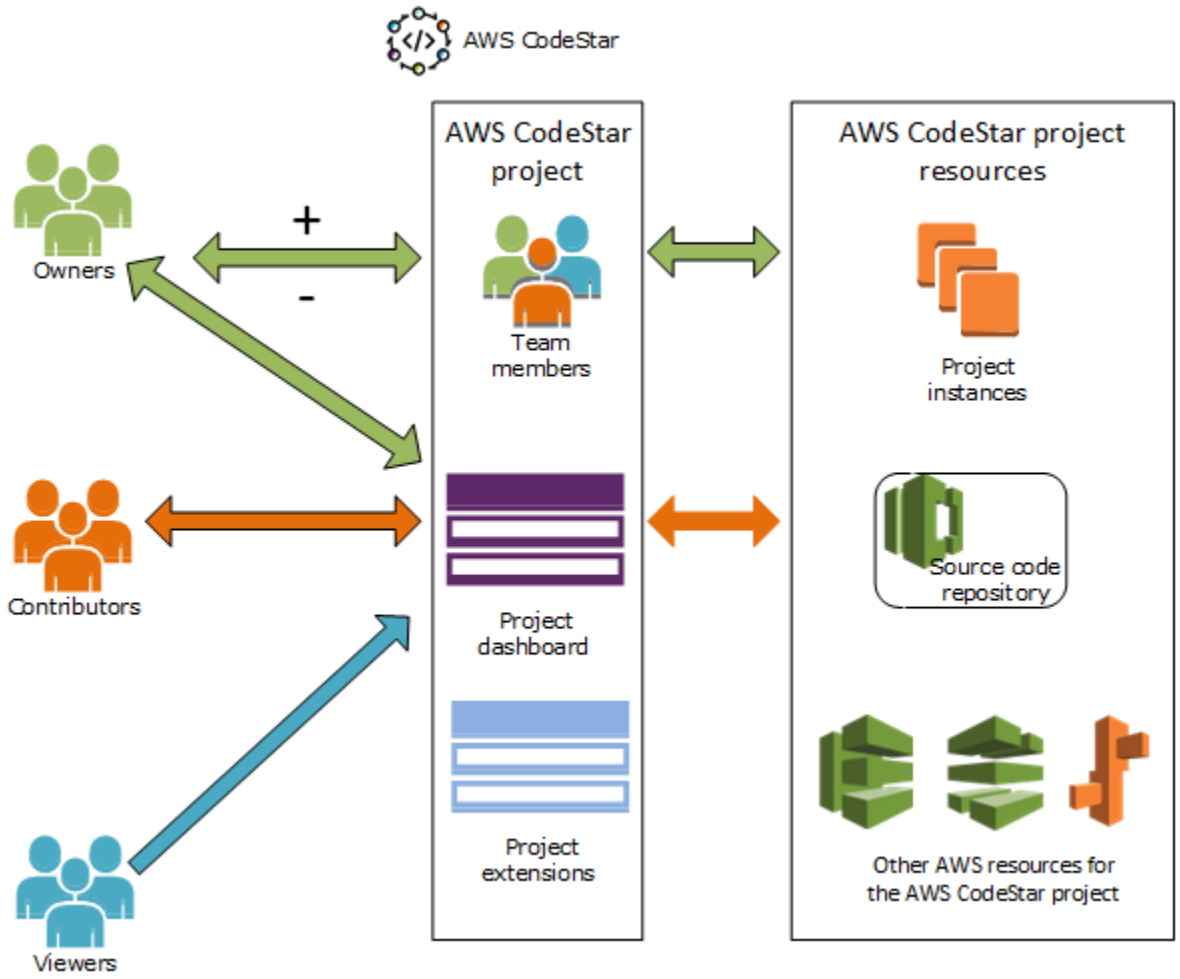
- 所有者: コードが CodeCommit に保存されている場合に、他のチームメンバーの追加および削除、プロジェクトリポジトリへのコードの投稿、プロジェクトに関連した Linux で実行されている Amazon EC2 インスタンスへの他のチームメンバーのリモートアクセスの許可および拒否、プロジェクトダッシュボードの設定、および、プロジェクトの削除ができます。
- 寄稿者: コードが CodeCommit に保存されている場合に、JIRA タイルなどのダッシュボードリソースの追加および削除、プロジェクトリポジトリへのコードの投稿、およびダッシュボードの十分な操作ができます。チームメンバーの追加または削除、リソースへのリモートアクセスの許可または拒否、および、プロジェクトの削除はできません。これは、ほとんどのチームメンバーに対して選択すべきロールです。

- 閲覧者: コードが CodeCommit に保存されている場合に、プロジェクトダッシュボード、コードの表示、およびダッシュボードタイルへのプロジェクトとリソースの状態の表示ができます。

> **Important**
>
> プロジェクトで 以外のリソース AWS (GitHub リポジトリや Atlassian JIRA の問題など) を使用している場合、それらのリソースへのアクセスはリソースプロバイダーによって制御されます AWS CodeStar。詳細については、リソースプロバイダのドキュメントを参照してください。
>
> AWS CodeStar プロジェクトにアクセスできるユーザーは誰でも、 AWS CodeStar コンソールを使用して、 の外部 AWS にあるがプロジェクトに関連するリソースにアクセスできます。
>
> AWS CodeStar では、プロジェクトチームのメンバーがプロジェクトの関連する AWS Cloud9 開発環境に自動的に参加することはできません。チームメンバーによる共有環境への参加を許可するには、「プロジェクトチームメンバーと AWS Cloud9 環境を共有する」を参照してください。

IAM ポリシーは、各プロジェクトロールに関連付けられています。このポリシーは、リソースを反映してプロジェクト用にカスタマイズされています。これらのポリシーの詳細については、「AWS CodeStar のアイデンティティベースのポリシーの例」を参照してください。

以下の図は、各ロールと AWS CodeStar プロジェクトの関係を示しています。



トピック

- AWS CodeStar プロジェクトにチームメンバーを追加する
- AWS CodeStar チームメンバーのアクセス許可を管理する
- AWS CodeStar プロジェクトからチームメンバーを削除する

AWS CodeStar プロジェクトにチームメンバーを追加する

AWS CodeStar プロジェクトに所有者ロールがある場合、または`AWSCodeStarFullAccess`ポリシーが IAM ユーザーに適用されている場合は、プロジェクトチームに他の IAM ユーザーを追加できます。これは、 AWS CodeStar ロール (所有者、寄稿者、またはビューワー) をユーザーに適用するシンプルなプロセスです。これらのロールはプロジェクトごとでカスタマイズされています。例えば、Project A の寄稿者チームメンバーは、Project B の寄稿者チームメンバーのリソースとは異なるリソースへのアクセス許可を持っている可能性があります。チームメンバーは、プロジェクトで 1

つのロールのみを持つことができます。チームメンバーを追加すると、ロールによって定義されたレベルでプロジェクトに直ちにかかわることができます。

AWS CodeStar ロールとチームメンバーシップの利点は次のとおりです。

- チームメンバーの IAM でアクセス許可を手動で設定する必要はありません。
- チームメンバーのプロジェクトへのアクセスレベルを簡単に変更できます。
- ユーザーは、チームメンバーである場合にのみ、 AWS CodeStar コンソールでプロジェクトにアクセスできます。
- プロジェクトへのユーザーアクセスは、ロールによって定義されます。

チームおよび AWS CodeStar ロールの詳細については、AWS CodeStar Teams の使用「」および「」を参照してくださいAWS CodeStar ユーザープロファイルの使用。

チームメンバーをプロジェクトに追加するには、プロジェクトの AWS CodeStar 所有者ロールまたはAWSCodeStarFullAccessポリシーが必要です。

> **Important**
>
> チームメンバーを追加しても、そのメンバーの 以外のリソースへのアクセスには影響しません AWS (GitHub リポジトリや Atlassian JIRA の問題など) 。これらのアクセス許可は、リソースプロバイダーによって制御されます AWS CodeStar。詳細については、リソースプロバイダのドキュメントを参照してください。
> AWS CodeStar プロジェクトにアクセスできるユーザーは誰でも、 AWS CodeStar コンソールを使用して、 AWS そのプロジェクト以外のリソースにアクセスできます。
> チームメンバーをプロジェクトに追加しても、そのメンバーはプロジェクトの関連する AWS Cloud9 開発環境に自動的に参加することはできません。チームメンバーによる共有環境への参加を許可するには、「プロジェクトチームメンバーと AWS Cloud9 環境を共有する」を参照してください。
> プロジェクトへのアクセス権をフェデレーティッドユーザーに付与するには、 AWS CodeStar 所有者、寄稿者、または表示者の管理ポリシーをフェデレーティッドユーザーによって引き受けられたロールに手動でアタッチする必要があります。詳細については、「へのフェデレーティッドユーザーアクセス AWS CodeStar」を参照してください。

トピック

- チームメンバーを追加する (コンソール)

- チームメンバーを追加および表示する (AWS CLI)

チームメンバーを追加する (コンソール)

AWS CodeStar コンソールを使用して、チームメンバーをプロジェクトに追加できます。追加するユーザーの IAM ユーザーがすでに存在する場合は、その IAM ユーザーを追加することができます。存在しない場合は、プロジェクトに追加する際、そのユーザーの IAM ユーザーを作成することができます。

チームメンバーを AWS CodeStar プロジェクトに追加するには (コンソール)

1. AWS CodeStar コンソールを https://console.aws.amazon.com/codestar/://https://https://https://https://https://https
2. ナビゲーションペインから、[Projects] (プロジェクト) を選択し、プロジェクトを選択します。
3. プロジェクトのサイドナビゲーションペインで、[Team] (チーム) を選択します。
4. [Team members] (チームメンバー) ページで、[Add team member] (チームメンバーの追加) を選択します。
5. [Choose user] (ユーザーを選択) で、次のいずれかを実行します：

   - 追加する人物の IAM ユーザーがすでに存在する場合は、その IAM ユーザーをリストから選択します。

   > **Note**
   >
   > 別の AWS CodeStar プロジェクトに既に追加されているユーザーは、既存の AWS CodeStar ユーザーリストに表示されます。

   プロジェクトロールで、このユーザーの AWS CodeStar ロール (所有者、寄稿者、または閲覧者) を選択します。これは AWS CodeStar プロジェクトレベルのロールで、プロジェクトの所有者によってのみ変更できます。IAM ユーザーに適用すると、ロールは AWS CodeStar プロジェクトリソースへのアクセスに必要なすべてのアクセス許可を提供します。コードが IAM の CodeCommit に保存されている場合の Git 認証情報の作成と管理に必要なポリシー、または IAM でユーザーの Amazon EC2 SSH キーをアップロードするのに必要なポリシーが適用されます。

> **Important**
>
> 該当のユーザーとしてコンソールにサインインしていない限り、IAM ユーザーの表示名または E メール情報を入力または変更することはできません。詳細については、「AWS CodeStar ユーザープロファイルの表示情報を管理する」を参照してください。

[Add team member] (チームメンバーの追加) を選択します。

- プロジェクトに追加する人物の IAM ユーザーが存在しない場合は、[Create new IAM user] (新規 IAM ユーザーを作成) を選択します。新しい IAM ユーザーを作成できる IAM コンソールにリダイレクトされます。詳細については、IAM ユーザーガイドの「IAM ユーザーの作成」を参照してください。 IAM ユーザーを作成したら、 AWS CodeStar コンソールに戻り、ユーザーのリストを更新し、作成した IAM ユーザーをドロップダウンリストから選択します。この新しいユーザーに適用する AWS CodeStar表示名、E メールアドレス、プロジェクトロールを入力し、チームメンバーの追加を選択します。

> **Note**
>
> 管理しやすいように、少なくとも 1 人のユーザーにプロジェクトの所有者ロールを割り当てます。

6. 新しいチームメンバーに、次の情報を送信します：

   - AWS CodeStar プロジェクトの接続情報。
   - ソースコードが CodeCommit に保存されている場合、ローカルコンピュータから CodeCommit リポジトリに [instructions for setting up access with Git credentials] (Git 認証情報でアクセスを設定する手順)。
   - AWS CodeStar ユーザープロファイルの使用 で説明されているように、ユーザーが表示名、E メールアドレス、公開 Amazon EC2 SSH キーを管理する方法についての情報。
   - ユーザーが AWS を使用するのは初めてで、そのユーザーのために IAM ユーザーを作成した場合のワンタイムパスワードと接続情報。このパスワードはユーザーの初回サインイン時に失効します。ユーザーは新しいパスワードを選択する必要があります。

チームメンバーを追加および表示する (AWS CLI)

を使用して AWS CLI 、チームメンバーをプロジェクトチームに追加できます。また、プロジェクト内のすべてのチームメンバーに関する情報を表示することもできます。

チームメンバーを追加するには

1. ターミナルまたはコマンドウィンドウを開きます。
2. `--project-id`、`-user-arn`、`--project-role` パラメータを指定して、associate-team-member コマンドを実行します。`--remote-access-allowed` または `--no-remote-access-allowed` パラメータを含めることによって、ユーザーがプロジェクトインスタンスにリモートアクセスできるかどうかを指定することもできます。例:

```
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
```

このコマンドは出力なしを返します。

すべてのチームメンバーを表示するには (AWS CLI)

1. ターミナルまたはコマンドウィンドウを開きます。
2. `--project-id` パラメータを指定して、list-team-members コマンドを実行します。例:

```
aws codestar list-team-members --project-id my-first-projec
```

このコマンドは、次のような出力を返します :

```
{
    "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"}
 ]
}
```

AWS CodeStar チームメンバーのアクセス許可を管理する

チームメンバーの AWS CodeStar ロールを変更することで、チームメンバーのアクセス許可を変更します。各チームメンバーは、 AWS CodeStar プロジェクト内の 1 つのロールにのみ割り当てることができますが、多くのユーザーを同じロールに割り当てることができます。 AWS CodeStar コンソールまたは を使用して AWS CLI アクセス許可を管理できます。

Important

チームメンバーのロールを変更するには、そのプロジェクトの AWS CodeStar 所有者ロールを持つか、`AWSCodeStarFullAccess`ポリシーを適用する必要があります。
チームメンバーのアクセス許可を変更しても、そのチームメンバーの 以外のリソースへのアクセスには影響しません AWS (GitHub リポジトリや Atlassian JIRA の問題など)。これらのアクセス権限可は AWS CodeStarではなく、リソースプロバイダによって制御されます。詳細については、リソースプロバイダのドキュメントを参照してください。
AWS CodeStar プロジェクトにアクセスできるユーザーは誰でも、 AWS CodeStar コンソールを使用して、 の外部にある AWS が、そのプロジェクトに関連するリソースにアクセスできます。
プロジェクトのチームメンバーのロールを変更しても、そのメンバーがプロジェクトの AWS Cloud9 開発環境に参加することを自動的に許可または禁止することはありません。チームメンバーによる共有環境への参加を許可または拒否するには、「プロジェクトチームメンバーと AWS Cloud9 環境を共有する」を参照してください。

プロジェクトに関連付けられた Amazon EC2 Linux インスタンスにリモートアクセスするアクセス許可をユーザーに付与することもできます。このアクセス許可を付与した後、ユーザーはすべてのチームプロジェクトで AWS CodeStar ユーザープロファイルに関連付けられた SSH パブリックキーをアップロードする必要があります。Linux インスタンスに正常に接続するには、ユーザーは、SSH を設定し、ローカルコンピュータ上にプライベートキーを設定する必要があります。

トピック

チームアクセス許可の管理 (コンソール)

AWS CodeStar コンソールを使用して、チームメンバーのロールを管理できます。チームメンバーがプロジェクトに関連付けられた Amazon EC2 インスタンスにリモートアクセスできるかどうかを管理することもできます。

チームメンバーのロールを変更するには

1. AWS CodeStar コンソールを https://console.aws.amazon.com/codestar/.com で開きます。
2. ナビゲーションペインから、[Projects] (プロジェクト) を選択し、プロジェクトを選択します。
3. プロジェクトのサイドナビゲーションペインで、[Team] (チーム) を選択します。
4. [Team members] (チームメンバー) ページで、チームメンバーを選択し、[Edit] (編集) を選択します。
5. プロジェクトロールで、このユーザーに付与する AWS CodeStar ロール (所有者、寄稿者、またはビューワー) を選択します。

   AWS CodeStar ロールとそのアクセス許可の詳細については、「」を参照してくださいAWS CodeStar Teams の使用。

   [Edit team member] (チームメンバーを編集) を選択します。

チームメンバーに Amazon EC2 インスタンスへのリモートアクセスのアクセス許可を付与するには

1. AWS CodeStar コンソールを https://console.aws.amazon.com/codestar/.com で開きます。
2. ナビゲーションペインから、[Projects] (プロジェクト) を選択し、プロジェクトを選択します。
3. プロジェクトのサイドナビゲーションペインで、[Team] (チーム) を選択します。
4. [Team members] (チームメンバー) ページで、チームメンバーを選択し、[Edit] (編集) を選択します。
5. [Allow SSH access to project instances] (プロジェクトインスタンスへの SSH アクセスを許可する) を選択して、[Edit team member] (チームメンバーの編集) を選択します。
6. (オプション) まだアップロードしていない場合は、 AWS CodeStar ユーザーの SSH パブリックキーをアップロードする必要があることをチームメンバーに通知します。詳細については、「AWS CodeStar ユーザープロファイルにパブリックキーを追加する」を参照してください。

チームアクセス許可の管理 (AWS CLI)

を使用して AWS CLI 、チームメンバーに割り当てられたプロジェクトロールを管理できます。同じ AWS CLI コマンドを使用して、そのチームメンバーがプロジェクトに関連付けられた Amazon EC2 インスタンスにリモートアクセスできるかどうかを管理できます。

チームメンバーのアクセス許可を管理するには

1. ターミナルまたはコマンドウィンドウを開きます。
2. `--project-id`、`-user-arn`、`--project-role` パラメータを指定して、update-team-member コマンドを実行します。`--remote-access-allowed` または `--no-remote-access-allowed` パラメータを含めることによって、ユーザーがプロジェクトインスタンスにリモートアクセスできるかどうかを指定することもできます。たとえば、John_Doe という名前の IAM ユーザーのプロジェクトロールを更新し、プロジェクト Amazon EC2 インスタンスへのリモートアクセスなしで閲覧者のアクセス許可に変更するには、次のようにします：

   ```
   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
   ```

   このコマンドは、次のような出力を返します：

   ```
   {
    "projectRole":"Viewer",
    "remoteAccessAllowed":false,
    "userArn":"arn:aws:iam::111111111111:user/John_Doe"
   }
   ```

AWS CodeStar プロジェクトからチームメンバーを削除する

AWS CodeStar プロジェクトからユーザーを削除すると、そのユーザーはプロジェクトリポジトリのコミット履歴に表示されますが、CodeCommit リポジトリやプロジェクトパイプラインなどの他のプロジェクトリソースにはアクセスできなくなります。(このルールの例外は、これらのリソースへのアクセスを許可する他のポリシーが適用されている IAM ユーザーです。) ユーザーはプロジェクトダッシュボードにアクセスできず、ユーザーが AWS CodeStar ダッシュボードに表示するプロジェクトのリストにプロジェクトが表示されなくなります。 AWS CodeStar コンソールまたは を使用して AWS CLI 、プロジェクトチームからチームメンバーを削除できます。

> **Important**
>
> プロジェクトからチームメンバーを削除すると、プロジェクト Amazon EC2 インスタンスへのリモートアクセスは拒否されますが、ユーザーのアクティブな SSH セッションは閉じられません。
> チームメンバーを削除しても、そのチームメンバーの 以外のリソースへのアクセスには影響しません AWS (GitHub リポジトリや Atlassian JIRA の問題など)。これらのアクセス許可は、リソースプロバイダーによって制御されます AWS CodeStar。詳細については、リソースプロバイダのドキュメントを参照してください。
> プロジェクトからチームメンバーを削除しても、そのチームメンバーの関連 AWS Cloud9 開発環境は自動的に削除されず、そのメンバーが招待された関連 AWS Cloud9 開発環境に参加できなくなります。開発環境を削除するには、「プロジェクトから AWS Cloud9 環境を削除する」を参照してください。チームメンバーによる共有環境への参加を拒否するには、「プロジェクトチームメンバーと AWS Cloud9 環境を共有する」を参照してください。

プロジェクトからチームメンバーを削除するには、そのプロジェクトの AWS CodeStar 所有者ロールを持っているか、`AWSCodeStarFullAccess`ポリシーをアカウントに適用する必要があります。

トピック

- チームメンバーを削除する (コンソール)
- チームメンバーを削除する (AWS CLI)

チームメンバーを削除する (コンソール)

AWS CodeStar コンソールを使用して、プロジェクトチームからチームメンバーを削除できます。

プロジェクトからチームメンバーを削除するには

1. AWS CodeStar コンソールを https://console.aws.amazon.com/codestar/://https://https://https://https://https
2. ナビゲーションペインから、[Projects] (プロジェクト) を選択し、プロジェクトを選択します。
3. プロジェクトのサイドナビゲーションペインで、[Team] (チーム) を選択します。
4. リポジトリの [Team members] (チームメンバー) ページで、チームメンバーを選択し、[Remove] (削除) を選択します。

チームメンバーを削除する (AWS CLI)

を使用して AWS CLI 、プロジェクトチームからチームメンバーを削除できます。

チームメンバーを削除するには

1. ターミナルまたはコマンドウィンドウを開きます。
2. disassociate-team-member および `--project-id` を指定して、`-user-arn` コマンドを実行します。例:

```
aws codestar disassociate-team-member --project-id my-first-projec --user-arn
 arn:aws:iam:111111111111:user/John_Doe
```

このコマンドは、次のような出力を返します：

```
{
    "projectId": "my-first-projec",
    "userArn": "arn:aws:iam::111111111111:user/John_Doe"
}
```

AWS CodeStar ユーザープロファイルの使用

AWS CodeStar ユーザープロファイルは IAM ユーザーに関連付けられています。このプロファイルには、所属するすべての AWS CodeStar プロジェクトで使用される表示名と E メールアドレスが含まれています。プロファイルに関連付けられる SSH パブリックキーをアップロードできます。このパブリックキーは、所属する AWS CodeStar プロジェクトに関連付けられた Amazon EC2 インスタンスに接続するときに使用する SSH パブリック/プライベートキーペアの一部です。

> **Note**
>
> これらのトピックの情報は、 AWS CodeStar ユーザープロファイルのみを対象としています。プロジェクトで 以外のリソース AWS (GitHub リポジトリや Atlassian JIRA の問題など) を使用している場合、それらのリソースプロバイダーは独自のユーザープロファイルを使用することがあります。これは、異なる設定を持つ可能性があります。詳細については、リソースプロバイダのドキュメントを参照してください。

トピック

AWS CodeStar ユーザープロファイルの表示情報を管理する

AWS CodeStar コンソールまたは を使用して AWS CLI 、ユーザープロファイルの表示名と E メールアドレスを変更できます。ユーザープロファイルはプロジェクト固有ではありません。これは IAM ユーザーに関連付けられ、 AWS リージョン内の自分が属する AWS CodeStar プロジェクト全体に適用されます。複数の AWS リージョンのプロジェクトに属している場合は、個別のユーザープロファイルがあります。

独自のユーザープロファイルは AWS CodeStar コンソールでのみ管理できます。`AWSCodeStarFullAccess` ポリシーがある場合は、 を使用して他のプロファイル AWS CLI を表示および管理できます。

> **Note**
>
> このトピックの情報は、 AWS CodeStar ユーザープロファイルのみを対象としています。プロジェクトで 以外のリソース AWS (GitHub リポジトリや Atlassian JIRA の問題など) を使用

している場合、それらのリソースプロバイダーは独自のユーザープロファイルを使用することがあります。これは、異なる設定を持つ可能性があります。詳細については、リソースプロバイダのドキュメントを参照してください。

トピック

- ユーザープロファイルの管理 (コンソール)
- ユーザープロファイルの管理 (AWS CLI)

ユーザープロファイルの管理 (コンソール)

チームメンバーであるプロジェクトに移動し、プロファイル情報を変更することで、 AWS CodeStar コンソールでユーザープロファイルを管理できます。ユーザープロファイルはプロジェクト固有ではなくユーザー固有であるため、ユーザープロファイルの変更は、自分がチームメンバーである AWS リージョンのすべてのプロジェクトに表示されます。

> **Important**
>
> コンソールでユーザーの表示情報を変更するには、その IAM ユーザーとしてサインインしている必要があります。プロジェクトの AWS CodeStar 所有者ロールを持つユーザーや`AWSCodeStarFullAccess`ポリシーが適用されたユーザーであっても、他のユーザーは表示情報を変更できません。

AWS リージョン内のすべてのプロジェクトで表示情報を変更するには

1. AWS CodeStar コンソールを https://console.aws.amazon.com/codestar/://https://https://https://https://https
2. ナビゲーションペインで [Projects] (プロジェクト) を選択し、自分がチームメンバーであるプロジェクトを選択します。
3. プロジェクトのサイドナビゲーションペインで、[Team] (チーム) を選択します。
4. [Team members] (チームメンバー) ページで、 IAM ユーザーを選択し、[Edit] (編集) を選択します。
5. 表示名か E メールアドレス、またはその両方を編集して、[Edit team member] (チームメンバーの編集) を選択します。

> **Note**
>
> 表示名と E メールアドレスが必須です。詳細については、「の制限 AWS CodeStar」を参照してください。

ユーザープロファイルの管理 (AWS CLI)

を使用して AWS CLI 、 でユーザープロファイルを作成および管理できます AWS CodeStar。を使用して AWS CLI 、ユーザープロファイル情報を表示したり、 AWS リージョンの AWS アカウント用に設定されたすべてのユーザープロファイルを表示したりすることもできます。

ユーザー AWS プロファイルを作成、管理、または表示するリージョンにプロファイルが設定されていることを確認します。

ユーザープロファイルを作成するには

1. ターミナルまたはコマンドウィンドウを開きます。
2. `user-arn`、`display-name`、`email-address` パラメータを指定して、create-user-profile コマンドを実行します。例:

```
aws codestar create-user-profile --user-arn arn:aws:iam:111111111111:user/
John_Stiles --display-name "John Stiles" --email-address "john_stiles@example.com"
```

このコマンドは、次のような出力を返します :

```
{
 "createdTimestamp":1.491439687681E9,"
 displayName":"John Stiles",
 "emailAddress":"john.stiles@example.com",
 "lastModifiedTimestamp":1.491439687681E9,
 "userArn":"arn:aws:iam::111111111111:user/Jane_Doe"
}
```

表示情報を確認するには

1. ターミナルまたはコマンドウィンドウを開きます。
2. `user-arn` パラメータを指定して、describe-user-profile コマンドを実行します。例:

```
aws codestar describe-user-profile --user-arn arn:aws:iam:111111111111:user/
Mary_Major
```

このコマンドは、次のような出力を返します：

```
{
 "createdTimestamp":1.490634364532E9,
 "displayName":"Mary Major",
 "emailAddress":"mary.major@example.com",
 "lastModifiedTimestamp":1.491001935261E9,
 "sshPublicKey":"EXAMPLE=",
 "userArn":"arn:aws:iam::111111111111:user/Mary_Major"
}
```

表示情報を変更するには

1. ターミナルまたはコマンドウィンドウを開きます。
2. user-arn パラメータ、および display-name や email-address パラメータなどの変更するパラメータを指定して、update-user-profile コマンドを実行します。たとえば、「Jane Doe」という表示名のユーザーが表示名を「Jane Mary Doe」に変更する場合は次のようにします：

```
aws codestar update-user-profile --user-arn arn:aws:iam:111111111111:user/Jane_Doe
 --display-name "Jane Mary Doe"
```

このコマンドは、次のような出力を返します：

```
{
 "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"
}
```

AWS アカウントの AWS リージョン内のすべてのユーザープロファイルを一覧表示するには

1. ターミナルまたはコマンドウィンドウを開きます。
2. aws codestar list-user-profiles コマンドを実行します。例:

```
aws codestar list-user-profiles
```

このコマンドは、次のような出力を返します：

```
{
  "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"
 }
  ]
}
```

AWS CodeStar ユーザープロファイルにパブリックキーを追加する

パブリック SSH キーは、作成および管理するパブリックキー/プライベートキーのペアの一部としてアップロードできます。この SSH パブリックキー/プライベートキーのペアを使用して、Linux を実行する Amazon EC2 インスタンスにアクセスします。プロジェクト所有者によってリモートアクセスのアクセス許可が付与されている場合は、プロジェクトに関連付けられているインスタンスにのみアクセスできます。 AWS CodeStar コンソールまたは を使用して AWS CLI 、パブリックキーを管理できます。

> **Important**
>
> AWS CodeStar プロジェクト所有者は、プロジェクト所有者、寄稿者、およびビューワーにプロジェクトの Amazon EC2 インスタンスへの SSH アクセスを許可できますが、SSH キーを設定できるのは個人 (所有者、寄稿者、またはビューワー) のみです。そのためには、ユーザーが、所有者、寄稿者、または閲覧者としてサインインしている必要があります。
> AWS CodeStar は AWS Cloud9 環境の SSH キーを管理しません。

トピック

ポリシーキーを管理する (コンソール)

コンソールでパブリックキーとプライベートキーのペアを生成することはできませんが、ローカルで作成し、 AWS CodeStar コンソールからユーザープロファイルの一部として追加または管理できます。

パブリック SSH キーを管理するには

1. 端末または Bash エミュレータのウィンドウから、ssh-keygen コマンドを実行して、ローカルコンピュータに SSH パブリックキーとプライベートキーのペアを生成します。Amazon EC2 で許可されている形式でキーを生成できます。受け入れ可能な形式については、[Importing Your Own Public Key to Amazon EC2] (独自のパブリックキーを Amazon EC2 にインポートする)

を参照してください。理想的には、SSH-2 RSA であるキーを OpenSSH 形式で生成し、2048 ビットを含めます。パブリックキーは、.pub 拡張子の付いたファイルに保存されます。

2. AWS CodeStar コンソールを https://console.aws.amazon.com/codestar/.com で開きます。

   自分がチームメンバーであるプロジェクトを選択します。

3. ナビゲーションペインで、[Team] (チーム) を選択します。
4. [Team members] (チームメンバー) ページで、IAM ユーザーの名前を探して、[Edit] (編集) を選択します。
5. [Edit team member] (チームメンバーの編集) ページの[Remote access] (リモートアクセス) で、[Allow SSH access to project instances] (プロジェクトインスタンスへの SSH アクセスを許可する) を有効にします。
6. [SSH Public Key] (SSH パブリックキー) ボックスで、パブリックキーを貼り付け、[Edit team member] (チームメンバーの編集) を選択します。

> **Note**
>
> このフィールドの古いキーを削除して新しいキーを貼り付けることで、パブリックキーを変更できます。パブリックキーを削除するには、このフィールドの内容を削除し、[Edit team member] (チームメンバーの編集) を選択します。

パブリックキーを変更または削除すると、ユーザープロファイルが変更されます。プロジェクトの変更はありません。キーはプロファイルに関連付けられているため、リモートアクセスが許可されているすべてのプロジェクトで変更または削除されます。

パブリックキーを削除すると、リモートアクセスが許可されたすべてのプロジェクトで Linux を実行するAmazon EC2 インスタンスへのアクセスが削除されます。ただし、そのキーを使用して開いている SSH セッションが閉じられることはありません。開いているセッションを閉じたことを確認します。

パブリックキーを管理する (AWS CLI)

を使用して AWS CLI 、ユーザープロファイルの一部として SSH パブリックキーを管理できます。

パブリックキーを管理するには

1. 端末または Bash エミュレータのウィンドウから、ssh-keygen コマンドを実行して、ローカルコンピュータに SSH パブリックキーとプライベートキーのペアを生成します。Amazon EC2 で許可されている形式でキーを生成できます。受け入れ可能な形式については、[Importing Your Own Public Key to Amazon EC2] (独自のパブリックキーを Amazon EC2 にインポートする) を参照してください。理想的には、SSH-2 RSA であるキーを OpenSSH 形式で生成し、2048 ビットを含めます。パブリックキーは、.pub 拡張子の付いたファイルに保存されます。
2. AWS CodeStar ユーザープロファイルで SSH パブリックキーを追加または変更するには、 `--ssh-public-key`パラメータを使用して update-user-profile コマンドを実行します。以下に例を示します。

```
aws codestar update-user-profile --user-arn arn:aws:iam:111111111111:user/Jane_Doe
 --ssh-key-id EXAMPLE1
```

このコマンドは、次のような出力を返します：

```
{
 "createdTimestamp":1.491439687681E9,
 "displayName":"Jane Doe",
 "emailAddress":"jane.doe@example.com",
 "lastModifiedTimestamp":1.491442730598E9,
 "sshPublicKey":"EXAMPLE1",
 "userArn":"arn:aws:iam::111111111111:user/Jane_Doe"
}
```

プライベートキーを使用して Amazon EC2 インスタンスに接続

Amazon EC2 キーペアをすでに作成していることを確認します。パブリックキーを のユーザープロファイルに追加します AWS CodeStar。キーペアを作成するには、「ステップ 4: AWS CodeStar プロジェクトの Amazon EC2 キーペアの作成」を参照してください。パブリックキーをユーザープロファイルに追加するには、このトピックの前半にある手順を参照してください。

プライベートキーを使用して Amazon EC2 Linux インスタンスに接続するには

1. AWS CodeStar コンソールでプロジェクトを開き、ナビゲーションペインでプロジェクトを選択します。

2. [Project Resources] (プロジェクトリソース) で、[Type] (種類) が [Amazon EC2] で [Name] (名前) が [instance] (インスタンス) で始まる行で、[ARN] リンクを選択します。
3. Amazon EC2 コンソールで、[Connect] (接続) を選択します。
4. [Connect To Your Instance] (インスタンスへ接続) ダイアログボックスの指示に従います。

   ユーザー名については、`ec2-user` を使用します。ユーザー名に誤りがある場合は、インスタンスに接続することはできません。

詳細については、Amazon EC2 ユーザーガイドの以下のリソースを参照してください。

- SSH を使用した Linux インスタンスへの接続
- PuTTY を使用した Windows から Linux インスタンスへの接続
- MindTerm を使用した Linux インスタンスへの接続

のセキュリティ AWS CodeStar

のクラウドセキュリティが最優先事項 AWS です。 AWS カスタマーは、最もセキュリティの影響を受けやすい組織の要件を満たすように構築されたデータセンターとネットワークアーキテクチャを活用できます。

セキュリティは、 AWS とユーザーの間で共有される責任です。責任共有モデルでは、これをクラウドのセキュリティおよびクラウド内のセキュリティと説明しています。

- クラウドのセキュリティ – クラウドで AWS AWS サービスを実行するインフラストラクチャを保護する AWS 責任があります。 AWS また、 では、安全に使用できるサービスも提供しています。サードパーティーの監査者は、AWS コンプライアンスプログラムコンプライアンスプログラム の一環として、当社のセキュリティの有効性を定期的にテストおよび検証。に適用されるコンプライアンスプログラムの詳細については AWS CodeStar、「コンプライアンスプログラムによる AWS 対象範囲内のサービスコンプライアンスプログラム」を参照してください。
- クラウド内のセキュリティ – お客様の責任は、使用する AWS サービスによって決まります。また、ユーザーは、データの機密性、会社の要件、適用される法律や規制など、その他の要因についても責任を負います。

このドキュメントは、 を使用する際の責任共有モデルの適用方法を理解するのに役立ちます AWS CodeStar。以下のトピックでは、セキュリティとコンプライアンスの目的 AWS CodeStar を達成するために を設定する方法を示します。また、 AWS CodeStar リソースのモニタリングや保護に役立つ他の AWS サービスの使用方法についても説明します。

でカスタムポリシーを作成し、アクセス許可の境界を使用する場合は AWS CodeStar、タスクの実行に必要なアクセス許可のみを付与し、ターゲットリソースへのアクセス許可の範囲を絞り込むことで、最小特権アクセスを確保します。他のプロジェクトのメンバーがプロジェクト内のリソースにアクセスできないようにするには、組織メンバーに AWS CodeStar プロジェクトごとに個別のアクセス許可を付与します。ベストプラクティスとして、各メンバーのプロジェクトアカウントを作成し、そのアカウントにロールベースのアクセス権を割り当てます。

例えば、 AWS Organizations で AWS Control Tower などのサービスを使用して、DevOps グループの下で各開発者ロールのアカウントをプロビジョニングできます。その後、それらのアカウントにアクセス許可を割り当てることができます。全体的なアクセス許可はアカウントに適用されますが、ユーザーはプロジェクト外のリソースへのアクセス権が制限されています。

マルチアカウント戦略を使用して AWS リソースへの最小特権アクセスを管理する方法の詳細については、AWS 「Control Tower ユーザーガイド」の「ランディングゾーンの AWS マルチアカウント戦略」を参照してください。

トピック

でのデータ保護 AWS CodeStar

責任 AWS 共有モデル、AWS CodeStar でのデータ保護に適用されます。このモデルで説明されているように、 AWS はすべての を実行するグローバルインフラストラクチャを保護する責任があります AWS クラウド。ユーザーは、このインフラストラクチャでホストされるコンテンツに対する管理を維持する責任があります。また、使用する「 AWS のサービス 」のセキュリティ設定と管理タスクもユーザーの責任となります。データプライバシーの詳細については、データプライバシーに関するよくある質問を参照してください。欧州でのデータ保護の詳細については、AWS セキュリティブログに投稿された AWS 責任共有モデルおよび GDPR のブログ記事を参照してください。

データ保護の目的で、認証情報を保護し AWS アカウント 、 AWS IAM アイデンティティセンターまたは AWS Identity and Access Management (IAM) を使用して個々のユーザーを設定することをお勧めします。この方法により、それぞれのジョブを遂行するために必要な権限のみが各ユーザーに付与されます。また、次の方法でデータを保護することもお勧めします:

- 各アカウントで多要素認証 (MFA) を使用します。
- SSL/TLS を使用して AWS リソースと通信します。TLS 1.2 が必須で、TLS 1.3 をお勧めします。
- で API とユーザーアクティビティのログ記録を設定します AWS CloudTrail。
- AWS 暗号化ソリューションと、 内のすべてのデフォルトのセキュリティコントロールを使用します AWS のサービス。
- Amazon Macie などの高度な管理されたセキュリティサービスを使用します。これらは、Amazon S3 に保存されている機密データの検出と保護を支援します。

- コマンドラインインターフェイスまたは API AWS を介して にアクセスするときに FIPS 140-3 検証済み暗号化モジュールが必要な場合は、FIPS エンドポイントを使用します。利用可能な FIPS エンドポイントの詳細については、「連邦情報処理規格 (FIPS) 140-3」を参照してください。

お客様の E メールアドレスなどの極秘または機密情報を、タグ、または [名前] フィールドなどの自由形式のテキストフィールドに含めないことを強くお勧めします。これは、コンソール、API、または SDK を使用して CodeStar AWS CLIまたは他の AWS のサービス を操作する場合も同様です。AWS SDKs タグ、または名前に使用される自由記述のテキストフィールドに入力したデータは、請求または診断ログに使用される場合があります。外部サーバーに URL を提供する場合、そのサーバーへのリクエストを検証できるように、認証情報を URL に含めないことを強くお勧めします。

でのデータの暗号化 AWS CodeStar

デフォルトでは、 はプロジェクトに関して保存する情報を AWS CodeStar 暗号化します。プロジェクト名、説明、ユーザーのメールなど、プロジェクト ID 以外はすべて保管時に暗号化されます。プロジェクト IDs に個人情報を入れないでください。 は、デフォルトで転送中の情報 AWS CodeStar も暗号化します。保管時の暗号化または転送中の暗号化について、お客様による対応は必要ありません。

AWS CodeStar のための Identity and Access Management

AWS Identity and Access Management (IAM) は、管理者が AWS リソースへのアクセスを安全に制御 AWS のサービス するのに役立つ です。IAM 管理者は、誰を認証 (サインイン) し、誰に AWS CodeStar リソースの使用を承認する (アクセス許可を付与する) かを管理します。IAM は、追加料金なしで使用できる AWS のサービス です。

トピック

対象者

AWS Identity and Access Management (IAM) の使用方法は、AWS CodeStar で行う作業によって異なります。

[Service user] (サービスユーザー) – AWS CodeStar サービスを使用してジョブを実行する場合は、必要な認証情報とアクセス許可を管理者が用意します。さらに多くの AWS CodeStar 機能を使用して作業を行う場合は、追加のアクセス許可が必要になることがあります。アクセスの管理方法を理解すると、管理者に適切な許可をリクエストするのに役に立ちます。AWS CodeStar の特徴にアクセスできない場合は、「AWS CodeStar のアイデンティティとアクセスのトラブルシューティング」を参照してください。

[Service administrator] (サービス管理者) – 社内の AWS CodeStar リソースを担当している場合は、通常、AWS CodeStar へのフルアクセスがあります。サービスのユーザーがどの AWS CodeStar 機能やリソースにアクセスするかを決めるのは管理者の仕事です。その後、IAM 管理者にリクエストを送信して、サービスユーザーの権限を変更する必要があります。このページの情報を点検して、IAM の基本概念を理解してください。会社で AWS CodeStar を使用して IAM を利用する方法の詳細については、「AWS CodeStar が IAM と連携する仕組み」を参照してください。

[IAM administrator] (IAM 管理者) – IAM 管理者は、AWS CodeStar へのアクセスを管理するポリシーの書き込み方法の詳細について確認する場合があります。IAM で使用できる AWS CodeStar アイデンティティベースのポリシーの例を表示するには、「AWS CodeStar のアイデンティティベースのポリシーの例」 を参照してください。

アイデンティティを使用した認証

認証は、ID 認証情報 AWS を使用して にサインインする方法です。として、IAM ユーザーとして AWS アカウントのルートユーザー、または IAM ロールを引き受けることによって、認証 (にサインイン AWS) される必要があります。

ID ソースを介して提供された認証情報を使用して、フェデレーティッド ID AWS として にサインインできます。 AWS IAM アイデンティティセンター （ IAM Identity Center) ユーザー、会社のシングルサインオン認証、Google または Facebook 認証情報は、フェデレーティッド ID の例です。フェデレーティッド ID としてサインインする場合、IAM ロールを使用して、前もって管理者により ID フェデレーションが設定されています。フェデレーション AWS を使用して にアクセスすると、間接的にロールを引き受けることになります。

ユーザーの種類に応じて、 AWS マネジメントコンソール または AWS アクセスポータルにサインインできます。へのサインインの詳細については AWS、 AWS サインイン ユーザーガイドの「 へのサインイン方法 AWS アカウント」を参照してください。

AWS プログラムで にアクセスする場合、 はソフトウェア開発キット (SDK) とコマンドラインインターフェイス (CLI) AWS を提供し、認証情報を使用してリクエストを暗号化して署名します。 AWS ツールを使用しない場合は、リクエストに自分で署名する必要があります。推奨される方法を使用してリクエストを自分で署名する方法の詳細については、IAM ユーザーガイドの AWS API リクエストの署名を参照してください。

使用する認証方法を問わず、追加セキュリティ情報の提供をリクエストされる場合もあります。例えば、 AWS では、多要素認証 (MFA) を使用してアカウントのセキュリティを向上させることをお勧めします。詳細については、「AWS IAM アイデンティティセンター ユーザーガイド」の「Multi-factor authentication」(多要素認証) および「IAM ユーザーガイド」の「AWSでの多要素認証 (MFA) の使用」を参照してください。

AWS アカウント ルートユーザー

を作成するときは AWS アカウント、アカウント内のすべての およびリソースへの AWS のサービス 完全なアクセス権を持つ 1 つのサインイン ID から始めます。この ID は AWS アカウント ルートユーザーと呼ばれ、アカウントの作成に使用した E メールアドレスとパスワードでサインインすることでアクセスできます。日常的なタスクには、ルートユーザーを使用しないことを強くお勧めします。ルートユーザーの認証情報は保護し、ルートユーザーでしか実行できないタスクを実行するときに使用します。ルートユーザーとしてサインインする必要があるタスクの完全なリストについては、IAM ユーザーガイドの「ルートユーザー認証情報が必要なタスク」を参照してください。

IAM ユーザーとグループ

IAM ユーザーは、1 人のユーザーまたはアプリケーションに対して特定のアクセス許可 AWS アカウント を持つ 内の ID です。可能であれば、パスワードやアクセスキーなどの長期的な認証情報を保有する IAM ユーザーを作成する代わりに、一時的な認証情報を使用することをお勧めします。ただし、IAM ユーザーでの長期的な認証情報が必要な特定のユースケースがある場合は、アクセスキーをローテーションすることをお勧めします。詳細については、「IAM ユーザーガイド」の「長期的な認証情報を必要とするユースケースのためにアクセスキーを定期的にローテーションする」を参照してください。

IAM グループは、IAM ユーザーの集団を指定するアイデンティティです。グループとしてサインインすることはできません。グループを使用して、複数のユーザーに対して一度に権限を指定できます。多数のユーザーグループがある場合、グループを使用することで権限の管理が容易になります。例えば、IAMAdmins という名前のグループを設定して、そのグループに IAM リソースを管理する許可を与えることができます。

ユーザーは、ロールとは異なります。ユーザーは 1 人の人または 1 つのアプリケーションに一意に関連付けられますが、ロールはそれを必要とする任意の人が引き受けるようになっています。ユーザーには永続的な長期の認証情報がありますが、ロールでは一時的な認証情報が提供されます。詳細については、「IAM ユーザーガイド」の「IAM ユーザー (ロールではなく) の作成が適している場合」を参照してください。

IAM ロール

IAM ロールは、特定のアクセス許可 AWS アカウント を持つ 内のアイデンティティです。これは IAM ユーザーに似ていますが、特定のユーザーには関連付けられていません。ロールを切り替える AWS マネジメントコンソール ことで、 で IAM ロールを一時的に引き受けることができます。ロールを引き受けるには、 または AWS API オペレーションを AWS CLI 呼び出すか、カスタム URL を使用します。ロールを使用する方法の詳細については、「IAM ユーザーガイド」の「IAM ロールの使用」を参照してください。

IAM ロールと一時的な認証情報は、次の状況で役立ちます:

- フェデレーションユーザーアクセス – フェデレーティッド ID に許可を割り当てるには、ロールを作成してそのロールの許可を定義します。フェデレーティッド ID が認証されると、その ID はロールに関連付けられ、ロールで定義されている許可が付与されます。フェデレーションの詳細については、「IAM ユーザーガイド」の「サードパーティーアイデンティティプロバイダー向けロールの作成」を参照してください。IAM Identity Center を使用する場合は、許可セットを設定します。アイデンティティが認証後にアクセスできるものを制御するため、IAM Identity Center は、権限セットを IAM のロールに関連付けます。アクセス許可セットの詳細については、「AWS IAM アイデンティティセンター User Guide」の「Permission sets」を参照してください。
- 一時的な IAM ユーザー権限 - IAM ユーザーまたはロールは、特定のタスクに対して複数の異なる権限を一時的に IAM ロールで引き受けることができます。
- クロスアカウントアクセス - IAM ロールを使用して、自分のアカウントのリソースにアクセスすることを、別のアカウントの人物 (信頼済みプリンシパル) に許可できます。クロスアカウントアクセス権を付与する主な方法は、ロールを使用することです。ただし、一部の では AWS のサービス、 (プロキシとしてロールを使用する代わりに) リソースに直接ポリシーをアタッチできます。クロスアカウントアクセスにおけるロールとリソースベースのポリシーの違いについては、「IAM ユーザーガイド」の「IAM でのクロスアカウントのリソースへのアクセス」を参照してください。
- クロスサービスアクセス — 一部の は他の の機能 AWS のサービス を使用します AWS のサービス。例えば、あるサービスで呼び出しを行うと、通常そのサービスによって Amazon EC2 でアプリケーションが実行されたり、Amazon S3 にオブジェクトが保存されたりします。サービスで

は、呼び出し元プリンシパルの許可、サービスロール、またはサービスリンクロールを使用してこれを行う場合があります。

- 転送アクセスセッション (FAS) – IAM ユーザーまたはロールを使用してアクションを実行すると AWS、プリンシパルと見なされます。一部のサービスを使用する際に、アクションを実行することで、別のサービスの別のアクションがトリガーされることがあります。FAS は、 を呼び出すプリンシパルのアクセス許可を AWS のサービス、ダウンストリームサービス AWS のサービス へのリクエストリクエストリクエストと組み合わせて使用します。FAS リクエストは、サービスが他の AWS のサービス またはリソースとのやり取りを完了する必要があるリクエストを受け取った場合にのみ行われます。この場合、両方のアクションを実行するためのアクセス許可が必要です。FAS リクエストを行う際のポリシーの詳細については、「転送アクセスセッション」を参照してください。
- サービスロール - サービスがユーザーに代わってアクションを実行するために引き受ける IAM ロールです。IAM 管理者は、IAM 内からサービスロールを作成、変更、削除できます。詳細については、「IAM ユーザーガイド」の「AWS のサービスにアクセス許可を委任するロールの作成」を参照してください。
- サービスにリンクされたロール – サービスにリンクされたロールは、 にリンクされたサービスロールの一種です AWS のサービス。サービスは、ユーザーに代わってアクションを実行するロールを引き受けることができます。サービスにリンクされたロールは に表示され AWS アカウント 、 サービスによって所有されます。IAM 管理者は、サービスリンクロールのアクセス許可を表示できますが、編集することはできません。

- Amazon EC2 で実行されているアプリケーション – IAM ロールを使用して、EC2 インスタンスで実行され、 AWS CLI または AWS API リクエストを行うアプリケーションの一時的な認証情報を管理できます。これは、EC2 インスタンス内でのアクセスキーの保存に推奨されます。EC2 インスタンスに AWS ロールを割り当て、そのすべてのアプリケーションで使用できるようにするには、インスタンスにアタッチされたインスタンスプロファイルを作成します。インスタンスプロファイルにはロールが含まれ、EC2 インスタンスで実行されるプログラムは一時的な認証情報を取得できます。詳細については、IAM ユーザーガイドのAmazon EC2 インスタンスで実行されるアプリケーションに IAM ロールを使用して許可を付与するを参照してください。

IAM ロールと IAM ユーザーのどちらを使用するかについては、IAM ユーザーガイドの(IAM ユーザーではなく) IAM ロールをいつ作成したら良いのか?を参照してください。

ポリシーを使用したアクセスの管理

でアクセスを制御する AWS には、ポリシーを作成し、ID AWS またはリソースにアタッチします。ポリシーは AWS 、アイデンティティまたはリソースに関連付けられているときにアクセス許可を

定義する のオブジェクトです。 は、プリンシパル (ユーザー、ルートユーザー、またはロールセッション) がリクエストを行うときに、これらのポリシー AWS を評価します。ポリシーでの権限により、リクエストが許可されるか拒否されるかが決まります。ほとんどのポリシーは JSON ドキュメント AWS として に保存されます。JSON ポリシードキュメントの構造と内容の詳細については、IAM ユーザーガイドの JSON ポリシー概要を参照してください。

管理者は JSON AWS ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどのリソースに対してどのような条件下でアクションを実行できるかということです。

デフォルトでは、ユーザーやロールに権限はありません。IAM 管理者は、リソースで必要なアクションを実行するための権限をユーザーに付与する IAM ポリシーを作成できます。その後、管理者はロールに IAM ポリシーを追加し、ユーザーはロールを引き受けることができます。

IAM ポリシーは、オペレーションの実行方法を問わず、アクションの許可を定義します。例えば、`iam:GetRole` アクションを許可するポリシーがあるとします。そのポリシーを持つユーザーは、 AWS マネジメントコンソール、、 AWS CLIまたは AWS API からロール情報を取得できます。

アイデンティティベースのポリシー

アイデンティティベースポリシーは、IAM ユーザーグループ、ユーザーのグループ、ロールなど、アイデンティティにアタッチできる JSON 許可ポリシードキュメントです。これらのポリシーは、ユーザーとロールが実行できるアクション、リソース、および条件をコントロールします。アイデンティティベースのポリシーを作成する方法については、「IAM ユーザーガイド」の「IAM ポリシーの作成」を参照してください。

アイデンティティベースのポリシーは、さらにインラインポリシーまたはマネージドポリシーに分類できます。インラインポリシーは、単一のユーザー、グループ、またはロールに直接埋め込まれています。管理ポリシーは、 内の複数のユーザー、グループ、ロールにアタッチできるスタンドアロンポリシーです AWS アカウント。管理ポリシーには、 AWS 管理ポリシーとカスタマー管理ポリシーが含まれます。マネージドポリシーまたはインラインポリシーのいずれかを選択する方法については、IAM ユーザーガイドのマネージドポリシーとインラインポリシーの比較を参照してください。

リソースベースのポリシー

リソースベースのポリシーは、リソースに添付する JSON ポリシードキュメントです。リソースベースのポリシーには例として、IAM ロールの信頼ポリシーや Amazon S3 バケットポリシーがあげられます。リソースベースのポリシーをサポートするサービスでは、サービス管理者はポリシーを使用して特定のリソースへのアクセスを制御できます。ポリシーがアタッチされているリソースの

場合、指定されたプリンシパルがそのリソースに対して実行できるアクションと条件は、ポリシーによって定義されます。リソースベースのポリシーでは、プリンシパルを指定する必要があります。プリンシパルには、アカウント、ユーザー、ロール、フェデレーティッドユーザー、または を含めることができます AWS のサービス。

リソースベースのポリシーは、そのサービス内にあるインラインポリシーです。リソースベースのポリシーでは、IAM の AWS マネージドポリシーを使用できません。

アクセスコントロールリスト (ACL)

アクセスコントロールリスト (ACL) は、どのプリンシパル (アカウントメンバー、ユーザー、またはロール) がリソースにアクセスするための許可を持つかを制御します。ACL はリソースベースのポリシーに似ていますが、JSON ポリシードキュメント形式は使用しません。

Amazon S3、 AWS WAF、および Amazon VPC は、ACLs。ACL の詳細については、「Amazon Simple Storage Service デベロッパーガイド」の「アクセスコントロールリスト (ACL) の概要」を参照してください。

その他のポリシータイプ

AWS は、追加のあまり一般的ではないポリシータイプをサポートしています。これらのポリシータイプでは、より一般的なポリシータイプで付与された最大の権限を設定できます。

- アクセス許可の境界 - アクセス許可の境界は、アイデンティティベースポリシーによって IAM エンティティ (IAM ユーザーまたはロール) に付与できる権限の上限を設定する高度な機能です。エンティティにアクセス許可の境界を設定できます。結果として得られる権限は、エンティティのアイデンティティベースポリシーとそのアクセス許可の境界の共通部分になります。`Principal` フィールドでユーザーまたはロールを指定するリソースベースのポリシーでは、アクセス許可の境界は制限されません。これらのポリシーのいずれかを明示的に拒否した場合、権限は無効になります。アクセス許可の境界の詳細については、「IAM ユーザーガイド」の「IAM エンティティのアクセス許可の境界」を参照してください。
- サービスコントロールポリシー (SCPs) – SCPsは、 の組織または組織単位 (OU) の最大アクセス許可を指定する JSON ポリシーです AWS Organizations。 AWS Organizations は、ビジネスが所有する複数の をグループ化して一元管理するためのサービス AWS アカウント です。組織内のすべての機能を有効にすると、サービスコントロールポリシー (SCP) を一部またはすべてのアカウントに適用できます。SCP は、各 を含むメンバーアカウントのエンティティのアクセス許可を制限します AWS アカウントのルートユーザー。Organizations と SCP の詳細については、「AWS Organizations ユーザーガイド」の「サービスコントロールポリシー (SCP)」を参照してください。

- セッションポリシー - セッションポリシーは、ロールまたはフェデレーションユーザーの一時的なセッションをプログラムで作成する際にパラメータとして渡す高度なポリシーです。結果としてセッションの権限は、ユーザーまたはロールのアイデンティティベースポリシーとセッションポリシーの共通部分になります。また、リソースベースのポリシーから権限が派生する場合もあります。これらのポリシーのいずれかを明示的に拒否した場合、権限は無効になります。詳細については、「IAM ユーザーガイド」の「セッションポリシー」を参照してください。

複数のポリシータイプ

1 つのリクエストに複数のタイプのポリシーが適用されると、結果として作成される権限を理解するのがさらに難しくなります。が複数のポリシータイプが関係する場合にリクエストを許可するかどうか AWS を決定する方法については、IAM ユーザーガイドの「ポリシー評価ロジック」を参照してください。

AWS CodeStar が IAM と連携する仕組み

IAM を使用して AWS CodeStar へのアクセスを管理する前に、AWS CodeStar で使用できる IAM 機能について理解しておく必要があります。AWS CodeStar およびその他の AWS のサービスが IAM と連携する方法の概要を把握するには、IAM ユーザーガイドのAWS 「IAM と連携する のサービス」を参照してください。

トピック

- AWS CodeStar アイデンティティベースのポリシー
- AWS CodeStar リソースベースのポリシー
- AWS CodeStar タグに基づく認可
- AWS CodeStar の IAM ロール
- AWS CodeStarに対する IAM ユーザーアクセス
- へのフェデレーティッドユーザーアクセス AWS CodeStar
- AWS CodeStar を使用した一時的な認証情報の使用
- サービスリンクロール
- サービスロール

AWS CodeStar アイデンティティベースのポリシー

IAM アイデンティティベースのポリシーでは、許可または拒否されたアクションとリソース、およびアクションが許可または拒否される条件を指定できます。 AWS CodeStar は、ユーザーに代わっ

て複数のアイデンティティベースのポリシーを作成します。これにより、 は AWS CodeStar プロジェクトの範囲内 AWS CodeStar でリソースを作成および管理できます。AWS CodeStar では、特定のアクション、リソース、および条件キーをサポートしています。JSON ポリシーで使用するすべての要素については、「IAM ユーザーガイド」の「IAM JSON ポリシー要素のリファレンス」を参照してください。

アクション

管理者は JSON AWS ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどのリソースに対してどのような条件下でアクションを実行できるかということです。

JSON ポリシーの `Action` 要素にはポリシー内のアクセスを許可または拒否するために使用できるアクションが記述されます。ポリシーアクションの名前は通常、関連付けられた AWS API オペレーションと同じです。一致する API オペレーションのない許可のみのアクションなど、いくつかの例外があります。また、ポリシーに複数のアクションが必要なオペレーションもあります。これらの追加アクションは依存アクションと呼ばれます。

このアクションは関連付けられたオペレーションを実行するためのアクセス許可を付与するポリシーで使用されます。

AWS CodeStar のポリシーアクションは、アクションの前に以下のプレフィックス `codestar:` を使用します。たとえば、指定された IAM ユーザーが AWS CodeStar プロジェクトの説明などのプロジェクトの属性を編集できるようにするには、次のポリシーステートメントを使用できます。

```
{
  "Version": "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "codestar:UpdateProject"
      ],
      "Resource" : "arn:aws:codestar:us-east-2:project/my-first-projec"
    }
  ]
}
```

ポリシーステートメントには`Action` または `NotAction` 要素を含める必要があります。AWS CodeStar は、このサービスで実行できるタスクを記述する独自のアクションのセットを定義します。

単一のステートメントに複数のアクションを指定するには、次のようにコンマで区切ります：

```
"Action": [
      "codestar:action1",
      "codestar:action2"
```

ワイルドカード (*) を使用して複数アクションを指定できます。例えば、List という単語で始まるすべてのアクションを指定するには、次のアクションを含めます：

```
"Action": "codestar:List*"
```

AWS CodeStar アクションのリストを表示するには、「IAM ユーザーガイド」 の 「AWS IoT によって定義されたアクション」を参照してください。

リソース

管理者は JSON AWS ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルが、どのリソースに対してどのような条件下でアクションを実行できるかということです。

Resource JSON ポリシー要素はアクションが適用されるオブジェクトを指定します。ステートメントにはResource または NotResource 要素を含める必要があります。ベストプラクティスとして、Amazon リソースネーム (ARN) を使用してリソースを指定します。これは、リソースレベルの許可と呼ばれる特定のリソースタイプをサポートするアクションに対して実行できます。

オペレーションのリスト化など、リソースレベルの権限をサポートしないアクションの場合は、ステートメントがすべてのリソースに適用されることを示すために、ワイルドカード (*) を使用します。

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

AWS CodeStar プロジェクトリソースには次の ARN があります。

```
arn:aws:codestar:region:account:project/resource-specifier
```

ARN の形式の詳細については、「Amazon リソースネーム (ARNs AWS 「サービス名前空間」を参照してください。

たとえば、次の例では、 AWS リージョン の AWS アカウント *my-first-projec* に登録された という名前111111111111の AWS CodeStar プロジェクトを指定しますus-east-2。

```
arn:aws:codestar:us-east-2:111111111111:project/my-first-projec
```

以下は、 AWS リージョン 111111111111の AWS アカウント my-proj に登録された名前で始まる AWS CodeStar プロジェクトを指定しますus-east-2。

```
arn:aws:codestar:us-east-2:111111111111:project/my-proj*
```

プロジェクトの一覧表示など、一部の AWS CodeStar アクションは、リソースでは実行できません。このような場合はワイルドカード *を使用する必要があります。

```
"LisProjects": "*"
```

AWS CodeStar リソースタイプとその ARN のリストを表示するには、「IAM ユーザーガイド」 の「AWS CodeStar で定義されるリソース」を参照してください。どのアクションで各リソースの ARN を指定できるかについては、「AWS CodeStar で定義されるアクション」を参照してください。

条件キー

AWS CodeStar にはサービス固有条件キーがありませんが、いくつかのグローバル条件キーの使用がサポートされています。すべての AWS グローバル条件キーを確認するには、IAM ユーザーガイドのAWS 「グローバル条件コンテキストキー」を参照してください。

例

AWS CodeStar アイデンティティベースのポリシーの例については、「AWS CodeStar のアイデンティティベースのポリシーの例」 を参照してください。

AWS CodeStar リソースベースのポリシー

AWS CodeStar はリソースベースのポリシーをサポートしていません。

AWS CodeStar タグに基づく認可

タグを AWS CodeStar プロジェクトにアタッチするか、AWS CodeStar へのリクエストでタグを渡すことができます。タグに基づいてアクセスを管理するには、codestar:ResourceTag/*key-*

name、aws:RequestTag/*key-name*、または aws:TagKeys の条件キーを使用して、ポリシーの [Condition element] (条件要素) でタグ情報を提供します。AWS CodeStar リソースのタグ付けの詳細については、「the section called “プロジェクトタグの操作”」を参照してください。

その AWS CodeStar プロジェクトのタグに基づいてプロジェクトへのアクセスを制限するためのアイデンティティベースのポリシーの例を表示するには、「」を参照してくださいタグに基づく AWS CodeStar プロジェクトの表示。

AWS CodeStar の IAM ロール

IAM ロールは、特定のアクセス許可を持つ AWS アカウントのエンティティです。

IAM ユーザー、フェデレーティッドユーザー、ルートユーザー、または引き受けたロール AWS CodeStar として を使用できます。適切なアクセス許可を持つすべてのユーザータイプは、リソースへのプロジェクトアクセス許可を管理できます AWS が、IAM ユーザーに対してプロジェクトアクセス許可を自動的に AWS CodeStar 管理します。IAM ポリシー および ロールは、プロジェクトロールに基づき、そのようなユーザーにアクセス許可を付与します。IAM コンソールを使用して、IAM ユーザーに割り当てる他のポリシー AWS CodeStar やその他のアクセス許可を作成できます。

たとえば、ユーザーに AWS CodeStar プロジェクトの表示を許可するが、変更は許可しないとします。この場合、ビューワーロールを持つ AWS CodeStar プロジェクトに IAM ユーザーを追加します。すべての AWS CodeStar プロジェクトには、プロジェクトへのアクセスを制御するのに役立つ一連のポリシーがあります。さらに、どのユーザーがアクセスできるかを制御できます AWS CodeStar。

AWS CodeStar アクセスは、IAM ユーザーとフェデレーティッドユーザーで異なる方法で処理されます。IAM ユーザーのみ、チームに追加することができます。プロジェクトへのアクセス許可を IAM ユーザーに付与するには、ユーザーをプロジェクトチームに追加して、ロールをユーザーに割り当てます。フェデレーティッドユーザーにプロジェクトへのアクセス許可を付与するには、 AWS CodeStar プロジェクトロールの 管理ポリシーをフェデレーティッドユーザーのロールに手動でアタッチします。

この表は、各タイプのアクセス権で利用できるツールについて説明しています。

アクセス許可の機能	IAM ユーザー	フェデレーティッドユーザー	ルートユーザー
Amazon EC2 および Elastic Beanstalk プロジェクトへのリモートアクセスに使用する SSH キーの管理	✓		
AWS CodeCommit SSH アクセス	✓		
によって管理される IAM ユーザーアクセス許可 AWS CodeStar	✓		
手動で管理されるプロジェクトのアクセス許可		✓	✓
ユーザーはチームメンバーとしてプロジェクトに追加することができます	✓		

AWS CodeStarに対する IAM ユーザーアクセス

プロジェクトに IAM ユーザーを追加して、ユーザーのロールを選択すると、 AWS CodeStar によって、適切なポリシーが IAM ユーザーに自動的に適用されます。IAM ユーザーは、IAM でポリシーやアクセス許可を直接アタッチまたは管理する必要はありません。IAM ユーザーを AWS CodeStar プロジェクトに追加する方法については、「」を参照してくださいAWS CodeStar プロジェクトにチームメンバーを追加する。 AWS CodeStar プロジェクトから IAM ユーザーを削除する方法については、「」を参照してくださいAWS CodeStar プロジェクトからチームメンバーを削除する。

インラインポリシーを IAM ユーザーにアタッチする

プロジェクトにユーザーを追加すると、 はユーザーのロールに一致するプロジェクトの管理ポリシー AWS CodeStar を自動的にアタッチします。プロジェクトの AWS CodeStar 管理ポリシーを IAM ユーザーに手動でアタッチしないでください。を除き`AWSCodeStarFullAccess`、 AWS CodeStar プロジェクトで IAM ユーザーのアクセス許可を変更するポリシーをアタッチすることはお勧めしません。独自のポリシーを作成してアタッチすることを決定した場合は、「IAM ユーザーガイド」 の 「IAM アイデンティティアクセス権限の追加と削除」 を参照してください。

へのフェデレーティッドユーザーアクセス AWS CodeStar

IAM ユーザーを作成するか、ルートユーザーを使用する代わりに、、エンタープライズユーザーディレクトリ AWS Directory Service、ウェブ ID プロバイダー、またはロールを引き受ける IAM ユーザーからユーザー ID を使用できます。このようなユーザーはフェデレーションユーザーと呼ばれます。

AWS CodeStar プロジェクトAWS CodeStar レベルのポリシーとアクセス許可で説明されている管理ポリシーをユーザーの IAM ロールに手動でアタッチして、フェデレーティッドユーザーにプロジェクトへのアクセスを許可します。がプロジェクトリソースと IAM ロール AWS CodeStar を作成した後、所有者、寄稿者、またはビューワーポリシーをアタッチします。

前提条件:

- ID プロバイダーを設定する必要があります。たとえば、SAML ID プロバイダーをセットアップし、プロバイダーを介した AWS 認証を設定できます。ID プロバイダーの設定の詳細については、「IAM ID プロバイダーの作成」を参照してください。SAML フェデレーションの詳細については、「SAML 2.0 ベースのフェデレーションについて」を参照してください。
- ID プロバイダーを通じてアクセスをリクエストする際に引き受けるフェデレーティッドユーザーのロールを作成済みである必要があります。フェデレーティッドユーザーがロールを引き受けられるように、STS 信頼ポリシーをロールに添付する必要があります。詳細については、「IAM ユーザーガイド」 の 「フェデレーティッドユーザーとロール」 を参照してください。
- AWS CodeStar プロジェクトを作成し、プロジェクト ID を知っている必要があります。

ID プロバイダーのロールの作成方法については、「サードパーティーの ID プロバイダー (フェデレーション) 用のロールの作成」を参照してください。

AWSCodeStarFullAccess 管理ポリシーをフェデレーティッドユーザーのロールに添付する

プロジェクトを作成するためのアクセス許可をフェデレーティッドユーザーに付与するには、`AWSCodeStarFullAccess` 管理ポリシーを添付します。これらのステップを実行するには、ルートユーザー、アカウントの管理者ユーザー、または `AdministratorAccess` 管理ポリシーか同等のポリシーに関連付けられている IAM ユーザーかフェデレーションユーザーとして、コンソールにサインイン済みである必要があります。

> **Note**
>
> プロジェクト作成後、プロジェクト所有者のアクセス許可は自動的に適用されません。「プロジェクトの AWS CodeStar Viewer/Contributor/Owner管理ポリシーをフェデレーティッドユーザーのロールにアタッチする」に示されているように、アカウントの管理者のアクセス許可を持つロールを使用して、所有者の管理ポリシーをアタッチします。

1. [IAM コンソール] を開きます。ナビゲーションペインで、[Policies] (ポリシー) を選択します。
2. 検索フィールドに「`AWSCodeStarFullAccess`」と入力します。ポリシータイプが [AWS managed] (マネージド) のポリシー名が表示されます。このポリシーを展開して、ポリシーステートメントのアクセス許可を参照することができます。
3. ポリシーの横にある円形を選択して、[Policy Actions] (ポリシーアクション) の [Attach] (添付) を選択します。
4. [Summary] (概要) ページで、 [Attached entities] (添付されたエンティティ) タブを選択します。[Attach] (添付) を選択します。
5. [Attach Policy] (ポリシーの添付) ページの検索フィールドで、フェデレーティッドユーザーのロールをフィルタリングします。ロールの名前の横にあるボックスを選択し、[Attach policy] (ポリシーの添付) を選択します。[Attached entities] (添付されたエンティティ) タブに、新しいアタッチメントが表示されます。

プロジェクトの AWS CodeStar Viewer/Contributor/Owner管理ポリシーをフェデレーティッドユーザーのロールにアタッチする

プロジェクトへのアクセス権をフェデレーティッドユーザーに付与するには、適切な所有者、寄稿者、閲覧者の管理ポリシーをユーザーのロールに添付します。管理ポリシーによって、適切なアクセス許可のレベルが指定されます。IAM ユーザーとは異なり、フェデレーティッドユーザーの管理ポリシーは手動でアタッチおよびデタッチする必要があります。これは、 のチームメンバーにプロジェクトアクセス許可を割り当てることと同じです AWS CodeStar。これらのステップを実行するには、ルートユーザー、アカウントの管理者ユーザー、または `AdministratorAccess` 管理ポリシーか同等のポリシーに関連付けられている IAM ユーザーかフェデレーションユーザーとして、コンソールにサインイン済みである必要があります。

前提条件:

- フェデレーティッドユーザーが引き受けるロールを作成しているか、既存のロールを設定されている必要があります。

- 付与するアクセス許可のレベルを把握しておく必要があります。所有者、寄稿者、閲覧者のロールに添付されている管理ポリシーは、プロジェクトのロールベースのアクセス許可を提供します。
- AWS CodeStar プロジェクトが作成されている必要があります。プロジェクトが作成されるまで、管理ポリシーは IAM で利用できません。

1. [IAM コンソール] を開きます。ナビゲーションペインで、[Policies] (ポリシー) を選択します。
2. 検索フィールドにプロジェクト ID を入力します。ポリシータイプが [Customer managed] (カスタマー管理) で、プロジェクトに一致するポリシー名が表示されます。このポリシーを展開して、ポリシーステートメントのアクセス許可を参照することができます。
3. これらのうち、いずれかの管理ポリシーを選択します。ポリシーの横にある円形を選択して、[Policy Actions] (ポリシーアクション) の [Attach] (添付) を選択します。
4. [Summary] (概要) ページで、 [Attached entities] (添付されたエンティティ) タブを選択します。[Attach] (添付) を選択します。
5. [Attach Policy] (ポリシーの添付) ページの検索フィールドで、フェデレーティッドユーザーのロールをフィルタリングします。ロールの名前の横にあるボックスを選択し、[Attach policy] (ポリシーの添付) を選択します。[Attached entities] (添付されたエンティティ) タブに、新しいアタッチメントが表示されます。

フェデレーティッドユーザーのロールから AWS CodeStar 管理ポリシーをデタッチする

AWS CodeStar プロジェクトを削除する前に、フェデレーティッドユーザーのロールにアタッチした管理ポリシーを手動でデタッチする必要があります。これらのステップを実行するには、ルートユーザー、アカウントの管理者ユーザー、または `AdministratorAccess` 管理ポリシーか同等のポリシーに関連付けられている IAM ユーザーかフェデレーションユーザーとして、コンソールにサインイン済みである必要があります。

1. [IAM コンソール] を開きます。ナビゲーションペインで、[Policies] (ポリシー) を選択します。
2. 検索フィールドにプロジェクト ID を入力します。
3. ポリシーの横にある円形を選択して、[Policy Actions] (ポリシーアクション) の [Attach] (添付) を選択します。
4. [Summary] (概要) ページで、 [Attached entities] (添付されたエンティティ) タブを選択します。
5. 検索フィールドで、フェデレーティッドユーザーのロールをフィルタリングします。[Detach] (デタッチ) を選択します。

フェデレーティッドユーザーのロールに AWS Cloud9 管理ポリシーをアタッチする

AWS Cloud9 開発環境を使用している場合は、 AWSCloud9User管理ポリシーをユーザーのロールにアタッチして、フェデレーティッドユーザーにその環境へのアクセスを許可します。IAM ユーザーとは異なり、フェデレーティッドユーザーの管理ポリシーは手動でアタッチおよびデタッチする必要があります。これらのステップを実行するには、ルートユーザー、アカウントの管理者ユーザー、または AdministratorAccess 管理ポリシーか同等のポリシーに関連付けられている IAM ユーザーかフェデレーションユーザーとして、コンソールにサインイン済みである必要があります。

前提条件:

- フェデレーティッドユーザーが引き受けるロールを作成しているか、既存のロールを設定されている必要があります。
- 付与するアクセス許可のレベルを把握しておく必要があります。
  - AWSCloud9User 管理ポリシーでは、ユーザーによる次の操作を許可します :
    - 独自の AWS Cloud9 開発環境を作成します。
    - 環境に関する情報を取得する。
    - 環境の設定を変更する。
  - AWSCloud9Administrator 管理ポリシーでは、自分自身または他のユーザーに対する次の操作をユーザーに許可します :
    - 環境を作成する。
    - 環境に関する情報を取得する。
    - 環境を削除する。
    - 環境の設定を変更する。

1. [IAM コンソール] を開きます。ナビゲーションペインで、[Policies] (ポリシー) を選択します。
2. 検索フィールドにポリシー名を入力します。ポリシータイプが AWS マネージドの管理ポリシーが表示されます。このポリシーを展開して、ポリシーステートメントのアクセス許可を参照することができます。
3. これらのうち、いずれかの管理ポリシーを選択します。ポリシーの横にある円形を選択して、[Policy Actions] (ポリシーアクション) の [Attach] (添付) を選択します。
4. [Summary] (概要) ページで、 [Attached entities] (添付されたエンティティ) タブを選択します。[Attach] (添付) を選択します。
5. [Attach Policy] (ポリシーの添付) ページの検索フィールドで、フェデレーティッドユーザーのロールをフィルタリングします。ロールの名前の横にあるボックスを選択し、[Attach Policy] (ポ

リシーの添付) を選択します。[Attached entities] (添付されたエンティティ) タブに、新しいアタッチメントが表示されます。

フェデレーティッドユーザーのロールから AWS Cloud9 管理ポリシーをデタッチする

AWS Cloud9 開発環境を使用している場合は、アクセスを許可するポリシーをデタッチすることで、フェデレーティッドユーザーのアクセスを削除できます。これらのステップを実行するには、ルートユーザー、アカウントの管理者ユーザー、または `AdministratorAccess` 管理ポリシーか同等のポリシーに関連付けられている IAM ユーザーかフェデレーションユーザーとして、コンソールにサインイン済みである必要があります。

1. [IAM コンソール] を開きます。ナビゲーションペインで、[Policies] (ポリシー) を選択します。
2. 検索フィールドにプロジェクト名を入力します。
3. ポリシーの横にある円形を選択して、[Policy Actions] (ポリシーアクション) の [Attach] (添付) を選択します。
4. [Summary] (概要) ページで、 [Attached entities] (添付されたエンティティ) タブを選択します。
5. 検索フィールドで、フェデレーティッドユーザーのロールをフィルタリングします。[Detach] (デタッチ) を選択します。

AWS CodeStar を使用した一時的な認証情報の使用

一時的な認証情報を使用して、フェデレーションでサインインする、IAM 役割を引き受ける、またはクロスアカウント役割を引き受けることができます。一時的なセキュリティ認証情報を取得するには、AssumeRole や GetFederationToken などの AWS STS API オペレーションを呼び出します。

AWS CodeStar は一時的な認証情報の使用をサポートしていますが、 AWS CodeStar チームメンバーの機能はフェデレーティッドアクセスでは機能しません。 AWS CodeStar チームメンバー機能は、チームメンバーとして IAM ユーザーの追加のみをサポートします。

サービスリンクロール

サービスにリンクされたロールを使用すると、 AWS サービスは他の サービスのリソースにアクセスして、ユーザーに代わってアクションを実行できます。サービスリンクロールは IAM アカウント内に表示され、サービスによって所有されます。 管理者は、サービスにリンクされたロールのアクセス許可を表示できますが、編集することはできません。

AWS CodeStar は、サービスにリンクされたロールをサポートしていません。

サービスロール

この機能により、ユーザーに代わってサービスがサービス役割を引き受けることが許可されます。この役割により、サービスがお客様に代わって他のサービスのリソースにアクセスし、アクションを完了することが許可されます。サービス役割はIAM アカウントに表示され、アカウントによって所有されます。つまり、 管理者は、このロールのアクセス許可を変更できます。ただし、それにより、サービスの機能が損なわれる場合があります。

AWS CodeStar は、サービスロールをサポートしています。 は、プロジェクトのリソースを作成および管理するときに、サービスロール aws-codestar-service-role AWS CodeStar を使用します。詳細については、「IAM ユーザーガイド」 の[ロールの主な用語と概念」を参照してください。

> **Important**
>
> このサービスロールを作成するには、 管理ユーザーまたはルートアカウントとしてサインインする必要があります。詳細については、「IAM ユーザーガイド」の「初回アクセスのみ: ルートユーザーの認証情報」および「最初の管理者ユーザーとグループを作成する」を参照してください。

このロールは、 でプロジェクトを初めて作成するときに作成されます AWS CodeStar。サービスロールは、ユーザーに代わって以下のことを行います :

- プロジェクト作成時に選択したリソースを作成する。
- これらのリソースに関する情報を AWS CodeStar プロジェクトダッシュボードに表示します。

また、プロジェクトのリソースを管理するときにも、ユーザーの代わりに機能します。このポリシーステートメントの例については、「AWSCodeStarServiceRole ポリシー」を参照してください。

さらに、 はプロジェクトタイプに応じて、プロジェクト固有のサービスロールを複数 AWS CodeStar 作成 CloudFormation します。ツールチェーンロールはプロジェクトタイプごとに作成されます。

- CloudFormation ロールを使用すると AWS CodeStar 、 にアクセスして CloudFormation 、 AWS CodeStar プロジェクトのスタックを作成および変更できます。
- ツールチェーンロールを使用すると AWS CodeStar 、 は他の AWS サービスにアクセスして、AWS CodeStar プロジェクトのリソースを作成および変更できます。

AWS CodeStar プロジェクトレベルのポリシーとアクセス許可

プロジェクトを作成すると、 はプロジェクトリソースを管理するために必要な IAM ロールとポリシー AWS CodeStar を作成します。ポリシーは 3 つのカテゴリに分類されます：

- プロジェクトのチームメンバー用の IAM ポリシー。
- ワーカーロール用の IAM ポリシー。
- ランタイム実行ロール用の IAM ポリシー。

チームメンバー用の IAM ポリシー。

プロジェクトを作成すると、 は所有者、寄稿者、およびビューワーがプロジェクトにアクセスするための 3 つのカスタマー管理ポリシー AWS CodeStar を作成します。すべての AWS CodeStar プロジェクトには、これら 3 つのアクセスレベルの IAM ポリシーが含まれています。これらのアクセスレベルはプロジェクト固有であり、標準名を持つ IAM 管理ポリシーで定義されます。ここで、*project-id* は AWS CodeStar プロジェクトの ID (*my-first-projec* など) です。

- `CodeStar_`*`project-id`*`_Owner`
- `CodeStar_`*`project-id`*`_Contributor`
- `CodeStar_`*`project-id`*`_Viewer`

> **Important**
>
> これらのポリシーは、 によって変更される可能性があります AWS CodeStar。手動では編集しないでください。アクセス許可を追加または変更する場合は、追加のポリシーを IAM ユーザーにアタッチします。

チームメンバー (IAM ユーザー) をプロジェクトに追加し、アクセスレベルを選択する際に、対応するポリシーが IAM ユーザーに添付され、プロジェクトリソースに対する一連の適切なアクセス許可がユーザーに付与されます。ほとんどの場合、IAM でポリシーまたはアクセス許可を直接アタッチまたは管理する必要はありません。 AWS CodeStar アクセスレベルポリシーを IAM ユーザーに手動でアタッチすることはお勧めしません。絶対に必要な場合は、 AWS CodeStar アクセスレベルポリシーの補足として、独自の管理ポリシーまたはインラインポリシーを作成して、独自のレベルのアクセス許可を IAM ユーザーに適用できます。

ポリシーの対象は、厳密にプロジェクトのリソースと特定のアクションになります。インフラストラクチャスタックに新しいリソースが追加されると、 AWS CodeStar は、サポートされているリソースタイプの 1 つである場合、新しいリソースへのアクセス許可を含めるようにチームメンバーポリシーを更新しようとします。

> **Note**
>
> AWS CodeStar プロジェクトのアクセスレベルのポリシーは、そのプロジェクトにのみ適用されます。これにより、ユーザーは自分のロールによって決定されるレベルで、アクセス許可を持つ AWS CodeStar プロジェクトのみを表示して操作できます。 AWS CodeStar プロジェクトを作成するユーザーのみが、プロジェクトに関係なく、すべての AWS CodeStar リソースへのアクセスを許可するポリシーを適用する必要があります。

すべての AWS CodeStar アクセスレベルポリシーは、アクセスレベルが関連付けられているプロジェクトに関連付けられた AWS リソースによって異なります。他の AWS サービスとは異なり、これらのポリシーは、プロジェクトのリソースの変更に応じてプロジェクトが作成および更新されたときにカスタマイズされます。したがって、正規の所有者、寄稿者、閲覧者の管理ポリシーはありません。

AWS CodeStar 所有者ロールポリシー

`CodeStar_project-id_Owner` カスタマー管理ポリシーでは、ユーザーは制限なしで AWS CodeStar プロジェクト内のすべてのアクションを実行できます。これは、ユーザーがチームメンバーを追加または削除することを許可する唯一のポリシーです。ポリシーの内容は、プロジェクトに関連付けられたリソースによって異なります。例については、「AWS CodeStar 所有者ロールポリシー」を参照してください。

このポリシーを持つ IAM ユーザーは、プロジェクト内のすべての AWS CodeStar アクションを実行できますが、`AWSCodeStarFullAccess`ポリシーを持つ IAM ユーザーとは異なり、プロジェクトを作成することはできません。アクセス`codestar:*`許可の範囲は、特定のリソース (その AWS CodeStar プロジェクト ID に関連付けられたプロジェクト) に限定されます。

AWS CodeStar 寄稿者ロールポリシー

`CodeStar_project-id_Contributor` カスタマー管理ポリシーは、プロジェクトに投稿してプロジェクトダッシュボードを変更することをユーザーに許可しますが、チームメンバーを追加または削除することは許可しません。ポリシーの内容は、プロジェクトに関連付けられたリソースによって異なります。例については、「AWS CodeStar 寄稿者ロールポリシー」を参照してください。

AWS CodeStar ビューワーロールポリシー

CodeStar_*project-id*_Viewer カスタマー管理ポリシーは、 AWS CodeStar内のプロジェクトを表示することをユーザーに許可しますが、リソースを変更したり、チームメンバーを追加または削除することは許可しません。ポリシーの内容は、プロジェクトに関連付けられたリソースによって異なります。例については、「AWS CodeStar ビューワーロールポリシー」を参照してください。

ワーカーロール用の IAM ポリシー

2018 年 12 月 6 日以降に AWS CodeStar プロジェクトを作成すると、AWS CodeStar は CodeStar-*project-id*-ToolChainと の 2 つのワーカーロールを作成しますCodeStar-*project-id*-CloudFormation。ワーカーロールは、 がサービスに渡すために AWS CodeStar 作成するプロジェクト固有の IAM ロールです。これにより、サービスがリソースを作成し、 AWS CodeStar プロジェクトのコンテキストでアクションを実行できるように、アクセス許可が付与されます。ツールチェーンワーカーロールには、CodeBuild、CodeDeploy、CodePipeline などのツールチェーンサービスと確立された信頼関係があります。プロジェクトのチームメンバー (所有者と寄稿者) には、信頼されたダウンストリームサービスにワーカーロールを渡すためのアクセス権が付与されます。このロールのインラインポリシーステートメントの例については、「AWS CodeStar ツールチェーンワーカーロールポリシー (2018 年 12 月 6 日以降の PDT)」を参照してください。

CloudFormation ワーカーロールには CloudFormation、 でサポートされている選択したリソースのアクセス許可と、アプリケーションスタックに IAM ユーザー、ロール、ポリシーを作成するアクセス許可が含まれます。また、 との信頼関係も確立されています CloudFormation。権限のエスカレーションや破壊的アクションのリスクを軽減するために、 CloudFormation ロールポリシーには、インフラストラクチャスタックで作成されたすべての IAM エンティティ (ユーザーまたはロール) にプロジェクト固有のアクセス許可の境界を要求する条件が含まれています。このロールのインラインポリシーステートメントの例については、「CloudFormation ワーカーロールポリシー」を参照してください。

2018 年 12 月 6 日より前に作成された AWS CodeStar プロジェクトの場合、PDT AWS CodeStar は CodePipeline、CodeBuild、CloudWatch Events などのツールチェーンリソースの個別のワーカーロールを作成し、また、限られたリソースセット CloudFormation をサポートする のワーカーロールを作成します。これらの各ロールには、対応するサービスとの間で確立された信頼関係があります。プロジェクトのチームメンバー (所有者、寄稿者) および他の一部のワーカーロールには、信頼されたダウンストリームサービスにロールを渡すためのアクセス権が付与されます。ワーカーロールのアクセス許可は、一連のプロジェクトリソースでロールが実行できる基本的なアクションのセットまで制限されたインラインポリシーで定義されます。これらのアクセス権限は静的です。作成時にプロジェクトに含まれるリソースへのアクセス許可が含まれますが、プロジェクトに新しいリソースが追

加されるときに更新されません。これらのポリシーステートメントの例については、以下を参照してください：

- CloudFormation ワーカーロールポリシー (2018 年 12 月 6 日より前)
- AWS CodePipeline ワーカーロールポリシー (2018 年 12 月 6 日より前)
- AWS CodeBuild ワーカーロールポリシー (2018 年 12 月 6 日より前)
- Amazon CloudWatch Events ワーカーロールポリシー (2018 年 12 月 6 日 (PDT) 以前)

実行ロールの IAM ポリシー

2018 年 12 月 6 日 (PDT) 以降に作成されたプロジェクトの場合、AWS CodeStar はアプリケーションスタックでサンプルプロジェクトの汎用実行ロールを作成します。このロールは、アクセス許可の境界ポリシーを使用してプロジェクトリソースに制限されます。サンプルプロジェクトを拡張すると、追加の IAM ロールを作成できます。 CloudFormation ロールポリシーでは、権限のエスカレーションを避けるために、アクセス許可の境界を使用してこれらのロールの範囲を絞り込む必要があります。詳細については、「IAM ロールをプロジェクトに追加する」を参照してください。

2018 年 12 月 6 日より前に作成された Lambda プロジェクトの場合、 は、プロジェクト AWS SAM スタック内のリソースを操作するアクセス許可を持つインラインポリシーがアタッチされた Lambda 実行ロール AWS CodeStar を作成します。SAM テンプレートに新しいリソースが追加されると、 は Lambda 実行ロールポリシーを更新 AWS CodeStar して、サポートされているリソースタイプの 1 つである場合に、新しいリソースへのアクセス許可を含めようとします。

IAM アクセス許可の境界

2018 年 12 月 6 日 (PDT) 以降、プロジェクトを作成すると、AWS CodeStar はカスタマー管理ポリシーを作成し、そのポリシーを IAM アクセス許可の境界 としてプロジェクト内の IAM ロールに割り当てます。AWS CodeStar では、アプリケーションスタックで作成されたすべての IAM エンティティにアクセス許可の境界が必要です。アクセス許可の境界により、ロールが持つことができる最大アクセス許可が管理されますが、アクセス許可を持つロールは提供されません。アクセス許可ポリシーにより、ロールのアクセス許可が定義されます。つまり、どれだけ多くのアクセス許可がロールに追加されても、そのロールを使用するすべてのユーザーは、アクセス許可の境界に含まれている以上のアクションを実行することはできません。アクセス許可ポリシーとアクセス許可の境界の評価方法の詳細については、「IAM ユーザーガイド」 の 「ポリシーの評価論理」を参照してください。の。

AWS CodeStar では、プロジェクト固有のアクセス許可の境界を使用して、プロジェクト外部のリソースへの権限のエスカレーションを防いでいます。AWS CodeStar アクセス許可の境界には、プ

ロジェクトリソースの ARN が含まれます。このポリシーステートメントの例については、「AWS CodeStar のアクセス許可の境界ポリシー」を参照してください。

AWS CodeStar 変換では、サポートされているリソースをアプリケーションスタック (`template.yml`) を通じてプロジェクトから追加または削除するときに、このポリシーが更新されます。

既存のプロジェクトへの IAM アクセス許可の境界の追加

2018 年 12 月 6 日 (PDT) 以前に作成された AWS CodeStar プロジェクトがある場合は、プロジェクトの IAM ロールに手動でアクセス許可を追加する必要があります。ベストプラクティスとして、プロジェクトのリソースのみを含むプロジェクト固有の境界を使用し、プロジェクト外部のリソースへの特権のエスカレーションを回避することをお勧めします。以下のステップに従って、プロジェクトの進化につれて更新される、AWS CodeStar で管理されたアクセス許可の境界を使用できます。

1. CloudFormation コンソールにサインインし、プロジェクト内のツールチェーンスタックのテンプレートを見つけます。このテンプレートは `awscodestar-`*`project-id`* という名前です。
2. このテンプレートを選択し、[Actions] (アクション) を選択して、[View/Edit template in Designer] (デザイナーでテンプレートを表示/編集) を選択します。
3. [`Resources`] セクションを見つけ、セクションの上部にある次のスニペットを含めます。

```
 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}-*'
```

CloudFormation コンソールからスタックを更新するには、追加の IAM アクセス許可が必要になる場合があります。

4. (オプション) アプリケーション固有の IAM ロールを作成する場合は、このステップを完了します。IAM コンソールから、プロジェクトの CloudFormation ロールにアタッチされているインラインポリシーを更新して、次のスニペットを含めます。ポリシーを更新するには、追加のIAM リソースが必要になる場合があります。

```
{
     "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. プロジェクトパイプラインを介して変更をプッシュし、AWS CodeStar が適切なアクセス許可を使用してアクセス許可の境界を更新するようにします。

詳細については、「IAM ロールをプロジェクトに追加する」を参照してください。

AWS CodeStar のアイデンティティベースのポリシーの例

デフォルトでは、IAM ユーザーおよびロールには、AWS CodeStar リソースを作成または変更するアクセス許可はありません。また、 AWS マネジメントコンソール、 AWS CLI、または AWS API を使用してタスクを実行することはできません。IAM 管理者は、指定されたリソースで特定の API 操作を実行するための許可をユーザーとロールに付与する IAM ポリシーを作成する必要があります。続いて、管理者はそれらの権限が必要な IAM ユーザーまたはグループにそのポリシーをアタッチする必要があります。

JSON ポリシードキュメントのこれらの例を使用して、IAM アイデンティティベースのポリシーを作成する方法については、「IAM ユーザーガイド」の「JSON タブでのポリシーの作成」を参照してください。

トピック

- ポリシーのベストプラクティス
- AWSCodeStarServiceRole ポリシー
- AWSCodeStarFullAccess ポリシー
- AWS CodeStar 所有者ロールポリシー
- AWS CodeStar 寄稿者ロールポリシー
- AWS CodeStar ビューワーロールポリシー
- AWS CodeStar ツールチェーンワーカーロールポリシー (2018 年 12 月 6 日以降の PDT)
- CloudFormation ワーカーロールポリシー
- CloudFormation ワーカーロールポリシー (2018 年 12 月 6 日より前)

- AWS CodePipeline ワーカーロールポリシー (2018 年 12 月 6 日より前)
- AWS CodeBuild ワーカーロールポリシー (2018 年 12 月 6 日より前)
- Amazon CloudWatch Events ワーカーロールポリシー (2018 年 12 月 6 日 (PDT) 以前)
- AWS CodeStar のアクセス許可の境界ポリシー
- プロジェクトのリソースの一覧表示
- AWS CodeStar コンソールの使用
- ユーザーが自分のアクセス許可を表示できるようにする
- AWS CodeStar プロジェクトの更新
- プロジェクトへのチームメンバーの追加
- AWS アカウントに関連付けられたユーザープロファイルの一覧表示
- タグに基づく AWS CodeStar プロジェクトの表示
- AWS CodeStar AWS 管理ポリシーの更新

ポリシーのベストプラクティス

ID ベースのポリシーは、ユーザーのアカウント内の AWS CodeStar リソースを誰かが作成、アクセス、または削除できるどうかを決定します。これらのアクションを実行すると、 AWS アカウントに料金が発生する可能性があります。アイデンティティベースポリシーを作成したり編集したりする際には、以下のガイドラインと推奨事項に従ってください:

- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行 – ユーザーとワークロードにアクセス許可の付与を開始するには、多くの一般的なユースケースにアクセス許可を付与するAWS 管理ポリシーを使用します。これらは で使用できます AWS アカウント。ユースケースに固有の AWS カスタマー管理ポリシーを定義することで、アクセス許可をさらに減らすことをお勧めします。詳細については、「IAM ユーザーガイド」の「AWS マネージドポリシー」または「ジョブ機能の AWS マネージドポリシー」を参照してください。
- 最小特権を適用する – IAM ポリシーで許可を設定する場合は、タスクの実行に必要な許可のみを付与します。これを行うには、特定の条件下で特定のリソースに対して実行できるアクションを定義します。これは、最小特権アクセス許可とも呼ばれています。IAM を使用して許可を適用する方法の詳細については、「IAM ユーザーガイド」の「IAM でのポリシーとアクセス許可」を参照してください。
- IAM ポリシーで条件を使用してアクセスをさらに制限する - ポリシーに条件を追加して、アクションやリソースへのアクセスを制限できます。例えば、ポリシー条件を記述して、すべてのリクエストを SSL を使用して送信するように指定できます。条件を使用して、サービスアクションが など

の特定の を通じて使用される場合に AWS のサービス、サービスアクションへのアクセスを許可することもできます CloudFormation。詳細については、「IAM ユーザーガイド」の「IAM JSON ポリシー要素:条件」を参照してください。

- IAM Access Analyzer を使用して IAM ポリシーを検証し、安全で機能的な権限を確保する - IAM Access Analyzer は、新規および既存のポリシーを検証して、ポリシーが IAM ポリシー言語 (JSON) および IAM のベストプラクティスに準拠するようにします。IAM アクセスアナライザーは 100 を超えるポリシーチェックと実用的な推奨事項を提供し、安全で機能的なポリシーの作成をサポートします。詳細については、IAM ユーザーガイドのIAM Access Analyzer ポリシーの検証を参照してください。
- 多要素認証 (MFA) を要求する – で IAM ユーザーまたはルートユーザーを必要とするシナリオがある場合は AWS アカウント、セキュリティを強化するために MFA を有効にします。API オペレーションが呼び出されるときに MFA を必須にするには、ポリシーに MFA 条件を追加します。詳細については、IAM ユーザーガイドのMFA 保護 API アクセスの設定を参照してください。

IAM でのベストプラクティスの詳細については、IAM ユーザーガイドのIAM でのセキュリティのベストプラクティスを参照してください。

AWSCodeStarServiceRole ポリシー

`aws-codestar-service-role` ポリシーは、 が他の サービスでアクションを実行 AWS CodeStar できるようにするサービスロールにアタッチされます。に初めてサインインするときは AWS CodeStar、サービスロールを作成します。一度だけ作成する必要があります。ポリシーは、作成後にサービスロールに自動的にアタッチされます。

```
{
    "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 ポリシー

AWS CodeStarのセットアップ の手順で、AWSCodeStarFullAccess という名前のポリシーを IAM ユーザーにアタッチしました。このポリシーステートメントにより、ユーザーは AWS アカウントに関連付けられた使用可能なすべてのリソース AWS CodeStar を使用して、 で使用可能な AWS CodeStar すべてのアクションを実行できます。これには、プロジェクトの作成と削除が含まれます。次の例は、代表的な AWSCodeStarFullAccess ポリシーのスニペットです。実際のポリシーは、新しい AWS CodeStar プロジェクトを開始するときに選択するテンプレートによって異なります。

ターゲットスタックなしで cloudformation::DescribeStacks を呼び出す場合、AWS CloudFormation では cloudformation::ListStacks アクセス許可が必要です。

アクセス許可の詳細

このポリシーには以下を実行するためのアクセス許可が含まれています。

- ec2– EC2 インスタンスに関する情報を取得して AWS CodeStar プロジェクトを作成します。
- cloud9– AWS Command Line Interface 環境に関する情報を取得します。
- cloudformation– AWS CodeStar プロジェクトスタックに関する情報を取得します。
- codestar– AWS CodeStar プロジェクト内でアクションを実行します。

```
{
  "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-*"
      ]
    }
  ]
}
```

ほとんどの場合、すべてのユーザーにこのような過剰なアクセス許可を付与することはありません。代わりに、 によって管理されるプロジェクトロールを使用して、プロジェクトレベルのアクセス許可を追加できます AWS CodeStar。ロールは AWS CodeStar 、プロジェクトへの特定のレベルのアクセスを許可し、次のように名前が付けられます。

- 所有者
- 寄稿者
- 表示者

AWS CodeStar 所有者ロールポリシー

AWS CodeStar 所有者ロールポリシーは、ユーザーが制限なしに AWS CodeStar プロジェクトですべてのアクションを実行することを許可します。AWS CodeStar は、所有者のアクセスレベルを持つプロジェクトチームのメンバーに、`CodeStar_`*`project-id`*`_Owner` ポリシーを適用します。

```
...
{
  "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"
  ]
}
...
```

AWS CodeStar 寄稿者ロールポリシー

AWS CodeStar 寄稿者のロールポリシーでは、ユーザーはプロジェクトに寄稿し、プロジェクトダッシュボードを変更することができます。AWS CodeStar は、寄稿者のアクセスレベルを持つプ

ロジェクトチームメンバーに CodeStar_*project-id*_Contributor ポリシーを適用します。寄稿者のアクセス権を持っているユーザーは、プロジェクトへの寄稿とダッシュボードの変更はできますが、チームメンバーの追加や削除はできません。

```
...
{
  "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 ビューワーロールポリシー

AWS CodeStar 閲覧者ロールポリシーでは、ユーザーが AWS CodeStar でプロジェクトを表示できます。AWS CodeStar は、閲覧者のアクセスレベルを持つプロジェクトチームメンバーに、CodeStar_*project-id*_Viewer ポリシーを適用します。閲覧者アクセス権を持っているユーザーは、AWS CodeStar 内のプロジェクトを表示できますが、リソースを変更したり、チームメンバーを追加または削除したりすることはできません。

```
...
{
  "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 ツールチェーンワーカーロールポリシー (2018 年 12 月 6 日以降の PDT)

2018 年 12 月 6 日以降に作成された AWS CodeStar プロジェクトの場合、AWS CodeStar は、他の AWS サービスでプロジェクトのリソースを作成するワーカーロールのインラインポリシーを作成します。ポリシーの内容は、作成するプロジェクトのタイプによって異なります。ポリシーの例を次に示します。詳細については、「ワーカーロール用の IAM ポリシー」を参照してください。

```
{
  "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"
    }
  ]
}
```

CloudFormation ワーカーロールポリシー

2018 年 12 月 6 日以降に作成された AWS CodeStar プロジェクトの場合、AWS CodeStar は AWS CodeStar プロジェクトの CloudFormation リソースを作成するワーカーロールのインラインポリシーを作成します。ポリシーの内容は、プロジェクトで必要なリソースのタイプによって異なります。ポリシーの例を次に示します。詳細については、「ワーカーロール用の IAM ポリシー」を参照してください。

```
{
{
    "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"
        }
    ]
}
```

CloudFormation ワーカーロールポリシー (2018 年 12 月 6 日より前)

AWS CodeStar プロジェクトが 2018 年 12 月 6 日より前に作成された場合、AWS CodeStar は CloudFormation ワーカーロールのインラインポリシーを作成しました。ポリシーステートメントの例を以下に示します。

```
{
    "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 ワーカーロールポリシー (2018 年 12 月 6 日より前)

2018 年 12 月 6 日 (PDT) 以前に作成されたAWS CodeStar プロジェクトの場合、AWS CodeStar は CodePipeline ワーカーロールのインラインポリシーを作成しました。ポリシーステートメントの例を以下に示します。

```
{
    "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 ワーカーロールポリシー (2018 年 12 月 6 日より前)

2018 年 12 月 6 日 (PDT) 以前に作成された AWS CodeStar プロジェクトの場合、AWS CodeStar は CodeBuild ワーカーロールのインラインポリシーを作成しました。ポリシーステートメントの例を以下に示します。

```
{
    "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"
        }
    ]
}
```

Amazon CloudWatch Events ワーカーロールポリシー (2018 年 12 月 6 日 (PDT) 以前)

2018 年 12 月 6 日 (PDT) 以前に作成された AWS CodeStar プロジェクトの場合、AWS CodeStar は CloudWatch Events ワーカーロールのインラインポリシーを作成しました。ポリシーステートメントの例を以下に示します。

```
{
    "Statement": [
        {
            "Action": [
                "codepipeline:StartPipelineExecution"
            ],
            "Resource": [
                "arn:aws:codepipeline:us-east-1:account-id:project-id-Pipeline"
            ],
            "Effect": "Allow"
        }
    ]
}
```

AWS CodeStar のアクセス許可の境界ポリシー

2018 年 12 月 6 日 (PDT) 以降に AWS CodeStar プロジェクトを作成すると、AWS CodeStar はプロジェクトのアクセス許可の境界ポリシーを作成します。このポリシーでは、プロジェクト外部のリソースへの特権のエスカレーションを防止できます。これは、プロジェクトの進化につれて更新される動的なポリシーです。ポリシーの内容は、作成するプロジェクトのタイプによって異なります。ポリシーの例を次に示します。詳細については、「IAM アクセス許可の境界」を参照してください。

```
{
  "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": [
        "*"
      ]
    }
  ]
}
```

プロジェクトのリソースの一覧表示

この例では、 AWS アカウントの指定された IAM ユーザーに、 AWS CodeStar プロジェクトのリソースを一覧表示するためのアクセス権を付与します。

```
{
  "Version": "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "codestar:ListResources",
      ],
      "Resource" : "arn:aws:codestar:us-east-2:project/my-first-projec"
    }
  ]
}
```

AWS CodeStar コンソールの使用

AWS CodeStar コンソールにアクセスするための特定のアクセス許可は必要ありませんが、AWSCodeStarFullAccessポリシーまたは AWS CodeStar プロジェクトレベルのロールの所有者、寄稿者、または閲覧者のいずれかがいない限り、何も便利なものはありません。AWSCodeStarFullAccess の詳細については、「AWSCodeStarFullAccess ポリシー」をご

参照ください。プロジェクトレベルのポリシーの詳細については、「チームメンバー用の IAM ポリシー。」を参照してください。

AWS CLI または AWS API のみを呼び出すユーザーには、最小限のコンソールアクセス許可を付与する必要はありません。代わりに、実行しようとしている API オペレーションに一致するアクションのみへのアクセスが許可されます。

ユーザーが自分のアクセス許可を表示できるようにする

この例では、ユーザーアイデンティティにアタッチされたインラインおよびマネージドポリシーの表示を IAM ユーザーに許可するポリシーの作成方法を示します。このポリシーには、コンソールで、または AWS CLI または AWS API を使用してプログラムでこのアクションを実行するアクセス許可が含まれています。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
```

```
        }
    ]
}
```

AWS CodeStar プロジェクトの更新

この例では、 AWS アカウントの指定された IAM ユーザーに、 AWS CodeStar プロジェクトの説明など、プロジェクトの属性を編集するためのアクセス権を付与します。

```
{
  "Version": "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "codestar:UpdateProject"
      ],
      "Resource" : "arn:aws:codestar:us-east-2:project/my-first-projec"
    }
  ]
}
```

プロジェクトへのチームメンバーの追加

この例では、指定された IAM ユーザーにプロジェクト ID *my-first-projec* を持つ AWS CodeStar プロジェクトにチームメンバーを追加する権限を付与しますが、そのユーザーにチームメンバーを削除する権限を明示的に拒否します。

```
{
  "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"
    }
      ]

  ]
}
```

AWS アカウントに関連付けられたユーザープロファイルの一覧表示

この例では、このポリシーがアタッチされている IAM ユーザーに、 AWS アカウントに関連付けられているすべての AWS CodeStar ユーザープロファイルを一覧表示することを許可します。

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

タグに基づく AWS CodeStar プロジェクトの表示

アイデンティティベースのポリシーの条件を使用して、タグに基づいて AWS CodeStar プロジェクトへのアクセスを管理できます。この例では、プロジェクトを表示できるポリシーを作成する方法を示します。ただし、プロジェクトタグ Owner にそのユーザーのユーザー名の値がある場合のみ、アクセス許可は付与されます。このポリシーでは、このアクションをコンソールで実行するために必要なアクセス許可も付与します。

```
{
    "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}"}
            }
        }
    ]
}
```

このポリシーをアカウントの IAM ユーザーにアタッチできます。richard-roe という名前のユーザーが AWS CodeStar プロジェクトを表示しようとする場合、プロジェクトに Owner=richard-roe または owner=richard-roe というタグが付いている必要があります。それ以外の場合、アクセスは拒否されます。条件キー名では大文字と小文字が区別されないため、条件タグキー Owner は Owner と owner の両方に一致します。詳細については、「IAM ユーザーガイド」の「IAM JSON ポリシー要素: 条件」を参照してください。

AWS CodeStar AWS 管理ポリシーの更新

このサービスがこれらの変更の追跡を開始してからの AWS CodeStar の AWS マネージドポリシーの更新に関する詳細を表示します。このページの変更に関する自動通知については、[Document history] (ドキュメントの履歴) ページの AWS CodeStar RSS フィードをサブスクライブしてください。

変更	説明	日付
AWSCodeStarFullAccess ポリシー — AWSCodeStarFullAccess ポリシーの更新	AWS CodeStar アクセスロールポリシーが更新されました。ポリシーの結果は同じですが、CloudFormation には DescribeStacks に加えて ListStacks が必要です。これはすでに必須になっています。	2023 年 3 月 24 日

変更	説明	日付
AWSCodeStarServiceRole ポリシー — AWSCodeStarServiceRole ポリシーの更新	AWS CodeStar サービスロールポリシーが更新され、ポリシーステートメント内の冗長アクションが修正されました。 サービスロールポリシーでは、AWS CodeStar サービスがユーザーに代わってアクションを実行できるようになります。	2021 年 9 月 23 日
AWS CodeStar は変更の追跡をスタートしました	AWS CodeStar は AWS 、管理ポリシーの変更の追跡を開始しました。	2021 年 9 月 23 日

AWS CodeStar のアイデンティティとアクセスのトラブルシューティング

次の情報は、AWS CodeStar と IAM の使用に伴って発生する可能性がある一般的な問題の診断や修復に役立ちます。

トピック

- AWS CodeStar でアクションを実行する権限がない
- iam:PassRole を実行する権限がない
- AWS 自分のアカウント以外のユーザーに AWS CodeStar リソースへのアクセスを許可したい

AWS CodeStar でアクションを実行する権限がない

アクションを実行する権限がないと から AWS マネジメントコンソール 通知された場合は、管理者に連絡してサポートを依頼してください。サインイン認証情報を提供した担当者が管理者です。

以下の例のエラーは、`mateojackson` IAM ユーザーがコンソールを使用して [`######`] の詳細を表示する際に、`codestar:GetWidget` 許可がない場合に発生します。

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

この場合、Mateo は、codestar:*GetWidget* アクションを使用して *my-example-widget* リソースへのアクセスが許可されるように、管理者にポリシーの更新を依頼します。

iam:PassRole を実行する権限がない

iam:PassRole アクションを実行する権限がないというエラーが表示された場合は、ポリシーを更新して AWS CodeStar にロールを渡せるようにする必要があります。

一部の AWS のサービス では、新しいサービスロールまたはサービスにリンクされたロールを作成する代わりに、そのサービスに既存のロールを渡すことができます。そのためには、サービスにロールを渡す権限が必要です。

以下の例のエラーは、marymajor という名前の IAM ユーザーがコンソールを使用して AWS CodeStar でアクションを実行しようする場合に発生します。ただし、このアクションをサービスが実行するには、サービスロールから付与された権限が必要です。メアリーには、ロールをサービスに渡す許可がありません。

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

この場合、Mary のポリシーを更新してメアリーに iam:PassRole アクションの実行を許可する必要があります。

サポートが必要な場合は、 AWS 管理者にお問い合わせください。サインイン認証情報を提供した担当者が管理者です。

AWS 自分のアカウント以外のユーザーに AWS CodeStar リソースへのアクセスを許可したい

他のアカウントのユーザーや組織外の人が、リソースにアクセスするために使用できるロールを作成できます。ロールの引き受けを委託するユーザーを指定できます。リソースベースのポリシーまたはアクセスコントロールリスト (ACL) をサポートするサービスの場合、それらのポリシーを使用して、リソースへのアクセスを付与できます。

詳細については、以下を参照してください：

- AWS CodeStar がこれらの機能をサポートしているかどうかを確認するには、「AWS CodeStar が IAM と連携する仕組み」を参照してください。
- 所有 AWS アカウント している のリソースへのアクセスを提供する方法については、IAM ユーザーガイドの「所有 AWS アカウント している別の の IAM ユーザーへのアクセスを提供する」を参照してください。
- リソースへのアクセスをサードパーティーに提供する方法については AWS アカウント、IAM ユーザーガイドの「サードパーティー AWS アカウント が所有する へのアクセスを提供する」を参照してください。
- ID フェデレーションを介してアクセスを提供する方法については、「IAM ユーザーガイド」の「外部で認証されたユーザー (ID フェデレーション) へのアクセスの許可」を参照してください。
- クロスアカウントアクセスにおけるロールとリソースベースのポリシーの使用方法の違いについては、「IAM ユーザーガイド」の「IAM でのクロスアカウントのリソースへのアクセス」を参照してください。

を使用した AWS CodeStar API コールのログ記録 AWS CloudTrail

AWS CodeStar は、ユーザー AWS CloudTrail、ロール、または のサービスによって実行されたアクションを記録する AWS サービスである と統合されています AWS CodeStar。CloudTrail は、 のすべての API コールをイベント AWS CodeStar としてキャプチャします。キャプチャされた呼び出しには、 AWS CodeStar コンソールからの呼び出しと AWS CodeStar API オペレーションへのコード呼び出しが含まれます。証跡を作成する場合は、イベントを含む S3 バケットへの CloudTrail イベントの継続的な配信を有効にすることができます AWS CodeStar。証跡を設定しない場合でも、CloudTrail コンソールの [イベント履歴] で最新のイベントを表示できます。CloudTrail によって収集された情報を使用して、リクエストの実行元の IP アドレス AWS CodeStar、リクエストの実行者、リクエストの実行日時などの詳細を確認できます。

CloudTrail の詳細については、「AWS CloudTrail ユーザーガイド」を参照してください。

AWS CodeStar CloudTrail の情報

CloudTrail は、 AWS アカウントの作成時にアカウントで有効になります。でアクティビティが発生すると AWS CodeStar、そのアクティビティは CloudTrail イベントとイベント履歴の他の AWS サービスイベントに記録されます。 AWS アカウントで最近のイベントを表示、検索、ダウンロードできます。詳細については、「CloudTrailイベント履歴でのイベントの表示」を参照してください。

のイベントなど、 AWS アカウントのイベントの継続的な記録については AWS CodeStar、証跡を作成します。デフォルトでは、コンソールで証跡を作成すると、証跡はすべての AWS リージョン

に適用されます。証跡は、 AWS パーティション内のすべてのリージョンからのイベントをログに記録し、指定した S3 バケットにログファイルを配信します。その他の AWS のサービスを設定して、CloudTrail ログで収集されたデータをより詳細に分析し、それに基づく対応を行うことができます。詳細については、次を参照してください:

- 証跡の作成のための概要
- CloudTrail がサポートするサービスと統合
- CloudTrail 用 Amazon SNS 通知の構成
- 「複数のリージョンからCloudTrailログファイルを受け取る」および「複数のアカウントからCloudTrailログファイルを受け取る」

すべての AWS CodeStar アクションは CloudTrail によってログに記録され、 AWS CodeStar API リファレンスに記載されています。例えば、`DescribeProject`、`UpdateProject`、`AssociateTeamMember` の各アクションを呼び出すと、CloudTrail ログファイルにエントリが生成されます。

各イベントまたはログエントリには、リクエストの生成者に関する情報が含まれます。同一性情報は次の判断に役立ちます。

- リクエストが、ルートと IAM ユーザー認証情報のどちらを使用して送信されたか。
- リクエストがロールまたはフェデレーションユーザーの一時的なセキュリティ認証情報を使用して行われたかどうか。
- リクエストが別の AWS サービスによって行われたかどうか。

詳細については、CloudTrail userIdentity 要素を参照してください。

AWS CodeStar ログファイルエントリについて

CloudTrail のログファイルは、単一か複数のログエントリを含みます。イベントは任意ソースからの単一リクエストを表し、リクエストされたアクション、アクションの日時、リクエストパラメータなどの情報を含みます。CloudTrail ログファイルは、パブリック API 呼び出しの順序付けられたスタックトレースではないため、特定の順序では表示されません。

次の例は、 AWS CodeStarで `CreateProject` オペレーションが呼び出されたことを示す CloudTrail ログエントリを示しています。

```
{
```

```
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROAJLIN2OF3UBEXAMPLE: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": "AROAJLIN2OF3UBEXAMPLE",
        "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"
}
```

のコンプライアンス検証 AWS CodeStar

AWS CodeStar は AWS コンプライアンスプログラムの対象ではありません。

特定のコンプライアンスプログラムの対象となる AWS サービスのリストについては、AWS 「コンプライアンスプログラムによる対象範囲内のサービス」を参照してください。一般的な情報については、「AWS コンプライアンスプログラム」を参照してください。

を使用して、サードパーティーの監査レポートをダウンロードできます AWS Artifact。詳細については、AWS 「Artifact でのレポートのダウンロード」を参照してください。

の耐障害性 AWS CodeStar

AWS グローバルインフラストラクチャは、 AWS リージョンとアベイラビリティーゾーンを中心に構築されています。 AWS リージョンは、低レイテンシー、高スループット、および冗長性の高いネットワークで接続された、物理的に分離された複数のアベイラビリティーゾーンを提供します。アベイラビリティーゾーンでは、アベイラビリティーゾーン間で中断せずに、自動的にフェイルオーバーするアプリケーションとデータベースを設計および運用することができます。アベイラビリティーゾーンは、従来の単一または複数のデータセンターインフラストラクチャよりも可用性、耐障害性、およびスケーラビリティが優れています。

AWS リージョンとアベイラビリティーゾーンの詳細については、AWS 「 グローバルインフラストラクチャ」を参照してください。

でのインフラストラクチャセキュリティ AWS CodeStar

マネージドサービスである AWS CodeStar は、 AWS グローバルネットワークセキュリティで保護されています。 AWS セキュリティサービスと がインフラストラクチャ AWS を保護する方法については、AWS 「 クラウドセキュリティ」を参照してください。インフラストラクチャセキュリティの

ベストプラクティスを使用して AWS 環境を設計するには、「Security Pillar AWS Well-Architected Framework」の「Infrastructure Protection」を参照してください。

AWS 公開された API コールを使用して、ネットワーク経由で CodeStar にアクセスします。クライアントは以下をサポートする必要があります。

- Transport Layer Security (TLS)。TLS 1.2 が必須で、TLS 1.3 をお勧めします。
- DHE (楕円ディフィー・ヘルマン鍵共有) や ECDHE (楕円曲線ディフィー・ヘルマン鍵共有) などの完全前方秘匿性 (PFS) による暗号スイート。これらのモードはJava 7 以降など、ほとんどの最新システムでサポートされています。

また、リクエストにはアクセスキー ID と、IAM プリンシパルに関連付けられているシークレットアクセスキーを使用して署名する必要があります。またはAWS Security Token Service (AWS STS) を使用して、一時的なセキュリティ認証情報を生成し、リクエストに署名することもできます。

デフォルトでは、 AWS CodeStar はサービストラフィックを分離しません。を使用して作成されたプロジェクト AWS CodeStar は、Amazon EC2、API Gateway、または Elastic Beanstalk を介してアクセス設定を手動で変更しない限り、パブリックインターネットで公開されます。これは意図的なものです。Amazon EC2、API Gateway、または Elastic Beanstalk のアクセス設定は、すべてのインターネットアクセスを禁止するなど、必要なレベルに変更できます。

AWS CodeStar では、デフォルトでは VPC エンドポイント (AWS PrivateLink) はサポートされませんが、プロジェクトリソースで直接サポートを設定できます。

の制限 AWS CodeStar

次の表は AWS CodeStar、プロジェクトリソースの他の AWS のサービス AWS CodeStar に依存する の制限を示しています。これらのサービスの制限を変更することができます。変更できる制限の詳細については、「AWS サービス制限」を参照してください。

プロジェクト数	1 つの AWS アカウントで最大 333 のプロジェクト。実際の上限は、他のサービスの依存性のレベル (例: AWS アカウントで許可される CodePipeline 内のパイプラインの最大数) によって異なります。
IAM ユーザーが属できる AWS CodeStar プロジェクトの数	個々の IAM ユーザーあたり最大 10 までです。
プロジェクト ID	プロジェクト IDsはアカウント内で一意である必要があります AWS 。プロジェクト ID は 2 文字以上にする必要があり、15 文字を超えることはできません。使用できる文字は次のとおりです。 a ~ z の文字。 0 ~ 9 の数字。 特殊文字 - (マイナス記号) 。 大文字、スペース、. (ピリオド) 、@ (アットマーク) 、_ (アンダースコア) などのその他の文字は許可されていません。
プロジェクト名	プロジェクト名の長さは 100 文字を超えることはできず、空白で開始または終了することはできません。
プロジェクトの説明	使用できる文字の組み合わせの長さは 0 ~ 1,024 文字です。プロジェクトの説明はオプションです。

AWS CodeStar プロジェクトのチームメンバー	100
ユーザープロファイルの表示名	使用できる文字の組み合わせの長さは 1 ~ 100 文字です。表示名は 1 文字以上にする必要があります。その文字にスペースは使用できません。表示名をスペースで開始または終了することはできません。
ユーザープロファイル内の E メールアドレス	E メールアドレスには @ が含まれ、有効なドメイン拡張で終わる必要があります。
フェデレーションアクセス、root アカウントへのアクセス、 AWS CodeStarへの一時アクセス	AWS CodeStar は、フェデレーティッドユーザーと一時的なアクセス認証情報の使用をサポートします。ルートアカウント AWS CodeStar で を使用することはお勧めしません。
IAM ロール	IAM ロールに添付されている管理ポリシーでは、最大 5,120 文字です。

トラブルシューティング AWS CodeStar

以下の情報は、 AWS CodeStarでの一般的な問題のトラブルシューティングに役立ちます。

トピック

プロジェクトの作成の失敗: プロジェクトが作成されませんでした

問題: プロジェクトを作成しようとすると、作成に失敗した旨のメッセージが表示されます。

解決方法: 失敗の最も一般的な原因は次のとおりです。

- その ID を持つプロジェクトは、別の AWS リージョンの AWS アカウント内に既に存在します。
- へのサインインに使用した IAM ユーザーには、プロジェクトの作成に必要なアクセス許可 AWS マネジメントコンソール がありません。
- AWS CodeStar サービスロールに必要なアクセス許可が 1 つ以上ありません。
- プロジェクトの 1 つ以上のリソースの上限に達した (IAM、Amazon S3 バケット、または CodePipeline のパイプラインのカスタマー管理ポリシーの制限など)。

プロジェクトを作成する前に、`AWSCodeStarFullAccess` ポリシーが IAM ユーザーに適用されていることを確認します。詳細については、「AWSCodeStarFullAccess ポリシー」を参照してください。

プロジェクトを作成するときは、ID が一意で、 AWS CodeStar 要件を満たしていることを確認します。AWS CodeStar お客様に代わって AWS リソースを管理するアクセス許可を に選択したことを確認してください。

その他の問題をトラブルシューティングするには、 CloudFormation コンソールを開き、作成しようとしたプロジェクトのスタックを選択し、イベントタブを選択します。1 つのプロジェクトに複数のスタックが存在する可能性があります。スタック名は `awscodestar-` で始まり、プロジェクト ID が続きます。スタックは [Deleted] (削除済み) フィルタービューにある場合があります。スタックイベント内のすべての失敗メッセージを確認し、失敗の原因としてリストされている問題を修正します。

プロジェクトの作成: プロジェクトの作成時に Amazon EC2 の設定を編集しようとするとエラーが発生します

問題: プロジェクトの作成中に Amazon EC2 の設定オプションを編集すると、エラーメッセージまたはグレイアウトされたオプションが表示され、プロジェクトの作成を続行できません。

解決方法: エラーメッセージの最も一般的な原因は次のとおりです :

- AWS CodeStar プロジェクトテンプレートの VPC (デフォルト VPC または Amazon EC2 設定の編集時に使用される VPC) には専用インスタンステナンシーがあり、専用インスタンスではインスタンスタイプはサポートされていません。別のインスタンスタイプ、または、別の Amazon VPC を選択します。
- AWS アカウントに Amazon VPCsがありません。デフォルトの VPC を削除し、他に作成していない。https://console.aws.amazon.com/vpc/ で、Amazon VPC コンソールを開き、[VPC] を選択

し、少なくとも 1 つの VPC が設定されていることを確認します。設定されていない場合は、作成します。詳細については、「Amazon VPC 入門ガイド」の「Amazon Virtual Private Cloud の概要」を参照してください。

- Amazon VPC にサブネットがない。別の VPC を選択するか、VPC のサブネットを作成します。詳細については、「VPC とサブネットの基本」を参照してください。

プロジェクトの削除: AWS CodeStar プロジェクトは削除されましたが、リソースはまだ存在します

問題： AWS CodeStar プロジェクトは削除されましたが、そのプロジェクト用に作成されたリソースはまだ存在します。デフォルトでは、プロジェクト AWS CodeStar が削除されると、 はプロジェクトリソースを削除します。バケットにデータが含まれている可能性があるため、ユーザーが [Delete resources] (リソースの削除) チェックボックスをオンにしても、一部のリソース (Amazon S3 バケットなど)は保持されます。

解決方法： CloudFormation コンソールを開き、プロジェクトの作成に使用される 1 つ以上の CloudFormation スタックを見つけます。スタック名は `awscodestar-` で始まり、プロジェクト ID が続きます。スタックは [Deleted] (削除済み) フィルタービューにある場合があります。スタックに関連付けられたイベントを確認し、プロジェクトに作成されたリソースを検出します。 AWS CodeStar プロジェクトを作成した AWS リージョン内のリソースごとに コンソールを開き、リソースを手動で削除します。

残っているプロジェクトリソースには次のようなものが含まれている場合があります：

- Amazon S3 の 1 つ以上のプロジェクトバケット。他のプロジェクトリソースとは異なり、Amazon S3 のプロジェクトバケットは、 AWS CodeStar プロジェクトとともに関連付けられた AWS リソースを削除チェックボックスがオンになっている場合、削除されません。

  https://console.aws.amazon.com/s3/ で Amazon S3 コンソールを開きます。
- CodeCommit のプロジェクトのソースリポジトリ。

  CodeCommit コンソールを https://console.aws.amazon.com/codecommit/://https://https://https://https://https://https://https://https
- CodePipeline のプロジェクトのパイプライン。

  https://console.aws.amazon.com/codepipeline/で、CodePipeline コンソールを開きます。
- CodeDeploy のアプリケーションおよび関連するデプロイグループ。

https://console.aws.amazon.com/codedeploy/ で、CodeDeploy コンソールを開きます。

- AWS Elastic Beanstalkのアプリケーションおよび関連する環境。

  https://console.aws.amazon.com/elasticbeanstalk/ で、Elastic Beanstalk コンソールを開きます。

- AWS Lambdaの関数。

  AWS Lambda コンソールを https://console.aws.amazon.com/lambda/://www.com で開きます。

- API Gateway の 1 つ以上の API。

  https://console.aws.amazon.com/apigateway で、API Gateway コンソールを開きます。

- 1 つ以上の IAM ポリシーまたは IAM のロール。

  にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/iam/:// www.com」で IAM コンソールを開きます。

- Amazon EC2 インスタンス。

  Amazon EC2 コンソール (https://console.aws.amazon.com/ec2/) を開きます。

- の 1 つ以上の開発環境 AWS Cloud9。

  開発環境を表示、アクセス、管理するには、 AWS Cloud9 コンソールを https://console.aws.amazon.com/cloud9/://https://www.https://www.https:// www.www.www.www.www.www.www.www.www.www.www.www.

プロジェクトで 以外のリソース AWS (GitHub リポジトリや Atlassian JIRA の問題など) を使用している場合、CodeStar プロジェクトとともに関連付けられたリソースを削除ボックスが選択されていても、それらの AWS リソースは削除されません。

チーム管理の失敗: IAM ユーザーを AWS CodeStar プロジェクトのチームに追加できませんでした

問題: プロジェクトにユーザーを追加しようとすると、追加に失敗したことを示すエラーメッセージが表示されます。

解決方法: このエラーの最も一般的な原因は、ユーザーが IAM でユーザーに適用できる管理ポリシーの制限に達していることです。また、ユーザーを追加しようとした AWS CodeStar プロジェクトに

所有者ロールがない場合、または IAM ユーザーが存在しないか削除された場合にも、このエラーが表示されることがあります。

その AWS CodeStar プロジェクトの所有者であるユーザーとしてサインインしていることを確認します。詳細については、「AWS CodeStar プロジェクトにチームメンバーを追加する」を参照してください。

他の問題のトラブルシューティングを行うには、IAM コンソールを開き、追加しようとしたユーザーを選択し、その IAM ユーザーに適用されている管理ポリシーの数を確認します。

詳細については、「IAM エンティティおよびオブジェクトの制限」を参照してください。変更できる制限の詳細については、「AWS サービスの制限」を参照してください。

アクセス失敗: フェデレーティッドユーザーが AWS CodeStar プロジェクトにアクセスできない

問題： フェデレーティッドユーザーが AWS CodeStar コンソールでプロジェクトを表示できない。

解決方法: フェデレーティッドユーザーとしてサインインしている場合は、サインインを引き受けるロールに適切な管理ポリシーが添付されていることを確認します。詳細については、「プロジェクトの AWS CodeStar Viewer/Contributor/Owner管理ポリシーをフェデレーティッドユーザーのロールにアタッチする」を参照してください。

ポリシーを手動でアタッチして、フェデレーティッドユーザーを AWS Cloud9 環境に追加します。「フェデレーティッドユーザーのロールに AWS Cloud9 管理ポリシーをアタッチする」を参照してください。

アクセスの失敗: フェデレーティッドユーザーが AWS Cloud9 環境にアクセスまたは作成できない

問題： フェデレーティッドユーザーがコンソールで AWS Cloud9 環境を表示または作成できない AWS Cloud9 。

解決方法: フェデレーティッドユーザーとしてサインインしている場合は、適切な管理ポリシーがフェデレーティッドユーザーのロールにアタッチされていることを確認します。

フェデレーティッドユーザーのロールにポリシーを手動でアタッチして、フェデレーティッドユーザーを AWS Cloud9 環境に追加します。「フェデレーティッドユーザーのロールに AWS Cloud9 管理ポリシーをアタッチする」を参照してください。

アクセスの失敗: フェデレーティッドユーザーは AWS CodeStar プロジェクトを作成できますが、プロジェクトリソースを表示できません

問題: フェデレーティッドユーザーは、プロジェクトを作成できたが、プロジェクトパイプラインなどのプロジェクトリソースを表示できない。

解決方法： **AWSCodeStarFullAccess**管理ポリシーをアタッチしている場合は、 でプロジェクトを作成するアクセス許可があります AWS CodeStar。ただし、すべてのプロジェクトリソースにアクセスするには、所有者の管理ポリシーをアタッチする必要があります。

がプロジェクトリソース AWS CodeStar を作成すると、すべてのプロジェクトリソースに対するプロジェクトアクセス許可が、所有者、寄稿者、および閲覧者管理ポリシーで利用可能になります。すべてのリソースにアクセスするには、所有者のポリシーをロールに手動でアタッチする必要があります。「ステップ 3: ユーザーの IAM アクセス許可を設定する」を参照してください。

サービスロールの問題: サービスロールを作成できませんでした

問題： でプロジェクトを作成しようとすると AWS CodeStar、サービスロールの作成を求めるメッセージが表示されます。作成するオプションを選択するとエラーが表示されます。

解決方法： このエラーの最も一般的な理由は、サービスロールを作成するのに十分なアクセス許可がないアカウント AWS で にサインインしていることです。 AWS CodeStar サービスロール (`aws-codestar-service-role`) を作成するには、管理ユーザーとして、またはルートアカウントでサインインする必要があります。コンソールからサインアウトし、`AdministratorAccess` 管理ポリシーが適用されている IAM ユーザーでサインインします。

サービスロールの問題: サービスロールが有効でないか、または存在しません

問題： AWS CodeStar コンソールを開くと、 AWS CodeStar サービスロールが欠落しているか無効であることを示すメッセージが表示されます。

解決方法: このエラーの最も一般的な原因は、管理ユーザーがサービスロール (`aws-codestar-service-role`) を編集または削除したことです。サービスロールが削除された場合は、作成する

よう求められます。管理ユーザーとして、またはルートアカウントでサインインし、ロールを作成する必要があります。ロールが編集された場合は、もはや有効ではありません。管理ユーザーとして IAM コンソールにサインインし、ロールのリストでサービスロールを見つけて削除します。 AWS CodeStar コンソールに切り替え、指示に従ってサービスロールを作成します。

プロジェクトロールの問題: AWS CodeStar プロジェクト内のインスタンスの AWS Elastic Beanstalk ヘルスステータスチェックが失敗する

問題： 2017 年 9 月 22 日より前に Elastic Beanstalk を含む AWS CodeStar プロジェクトを作成した場合、Elastic Beanstalk のヘルスステータスチェックが失敗する可能性があります。プロジェクト作成後 Elastic Beanstalk 設定を変更していない場合、ヘルスステータスチェックは失敗し、灰色の状態がレポートされます。ヘルスチェックの失敗にもかかわらず、アプリケーションは正常に実行します。プロジェクト作成後、Elastic Beanstalk 設定を変更した場合は、ヘルスステータスチェックが失敗するだけでなく、アプリケーションは正常に実行されない可能性があります。

修正: 1 つ以上の IAM ロールで、必要な IAM ポリシーステートメントが不足しています。不足しているポリシーを AWS アカウントの影響のあるロールに追加します。

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/iam/:// www.com」で IAM コンソールを開きます。

   （ これができない場合は、 AWS アカウント管理者にお問い合わせください ）。
2. ナビゲーションペインで Roles (ロール) を選択します。
3. ロールのリストで、[CodeStarWorker-***Project-ID***-EB] を選択します。ここで、*Project-ID* は、影響を受けるいずれかのプロジェクトの ID です。(リストでロールを見つけるのが困難な場合は、ロールの名前の一部またはすべてを [検索] ボックスに入力します。)
4. [Permissions] (アクセス許可) タブで [Attach Policy] (ポリシーの添付) を選択します。
5. ポリシーのリストで、[AWSElasticBeanstalkEnhancedHealth] および [AWSElasticBeanstalkService] を選択します。(リストでポリシーを見つけるのが困難な場合は、ポリシーの名前の一部またはすべてを [検索] ボックスに入力します。)
6. [Attach Policy] (ポリシーの添付) を選択します。
7. 名前が [CodeStarWorker-***Project-ID***-EB] パターンで、影響を受けるロールごとに、ステップ 3 ~ 6 を繰り返します。

プロジェクトロールの問題: プロジェクトロールが有効でないか、または存在しません

問題: プロジェクトにユーザーを追加しようとすると、プロジェクトロールのポリシーが存在しないか、または無効であるため、追加に失敗したことを示すエラーメッセージが表示されます。

解決方法: このエラーの最も一般的な原因は、1 つ以上のプロジェクトポリシーが編集または IAM から削除されたことです。プロジェクトポリシーは AWS CodeStar プロジェクトに固有であり、再作成することはできません。プロジェクトは使用できません。でプロジェクトを作成し AWS CodeStar、新しいプロジェクトにデータを移行します。使用できないプロジェクトのリポジトリからプロジェクトコードをクローンし、そのコードを新しいプロジェクトのリポジトリにプッシュします。チームの wiki 情報を古いプロジェクトから新しいプロジェクトにコピーします。新しいプロジェクトにユーザーを追加します。すべてのデータと設定を移行したら、使用できないプロジェクトを削除します。

プロジェクトの拡張機能: JIRA に接続できません

問題： Atlassian JIRA 拡張機能を使用して AWS CodeStar プロジェクトを JIRA インスタンスに接続しようとすると、「URL は有効な JIRA URL ではありません。URL が正しいことを確認してください。」

解決方法:

- JIRA URL が正しいことを確認してから、再接続を試みます。
- お客様のセルフホスト型の JIRA インスタンスは、公開インターネットからアクセスできない可能性があります。ネットワーク管理者に連絡して、公共のインターネットから JIRA インスタンスにアクセスできることを確認してから、再度接続してみてください。

GitHub: リポジトリのコミット履歴、課題、またはコードにアクセスできない

問題:GitHub にコードを保存するプロジェクトのダッシュボードで、[Commit history] (コミット履歴) および [GitHub Issues] (GitHub の課題) タイルに接続エラーが表示されるか、これらのタイルの [Open in GitHub] (GitHub で開く) または [Create issue] (課題を作成) にエラーが表示されます。

考えられる原因:

- AWS CodeStar プロジェクトが GitHub リポジトリにアクセスできなくなる可能性があります。
- GitHub でリポジトリが削除されたか名前が変更された可能性があります。

AWS CloudFormation: アクセス許可の不足により、スタックの作成がロールバックされた

リソースを `template.yml` ファイルに追加したら、 AWS CloudFormation スタック更新を表示して、エラーメッセージがないか確認します。特定の条件が満たされない場合、スタック更新は失敗します (例：必要なリソースに対するアクセス許可が不足している)。

> **Note**
>
> 2019 年 5 月 2 日をもって、既存のすべてのプロジェクトの CloudFormation ワーカーロールポリシーが更新されました。この更新により、プロジェクトパイプラインに付与されるアクセス権限の範囲が減り、プロジェクトのセキュリティが向上します。

トラブルシューティングを行うには、プロジェクトのパイプラインの AWS CodeStar ダッシュボードビューで障害ステータスを表示します。

次に、パイプラインのデプロイステージで CloudFormation リンクを選択して、 AWS CloudFormation コンソールで障害をトラブルシューティングします。スタック作成の詳細を表示するには、プロジェクトの [Events] (イベント) リストを展開し、障害メッセージがあれば表示します。このメッセージによって、不足しているアクセス許可が分かります。 CloudFormation ワーカーロールポリシーを修正してから、パイプラインを再実行します。

AWS CloudFormation Lambda 実行ロールで iam:PassRole を実行する権限がありません

Lambda 関数を作成するプロジェクトが 2018 年 12 月 6 日より前に作成された場合は、次のような CloudFormation エラーが表示されることがあります。

```
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)
```

このエラーは、 CloudFormation ワーカーロールに新しい Lambda 関数をプロビジョニングするためのロールを渡すアクセス許可がないために発生します。

このエラーを修正するには、次のスニペットを使用して CloudFormation ワーカーロールポリシーを更新する必要があります。

```
{
        "Action":[ "iam:PassRole" ],
        "Resource": [
           "arn:aws:iam::account-id:role/CodeStarWorker-project-id-Lambda",
           ],

        "Effect": "Allow"
}
```

ポリシーを更新したら、パイプラインを再実行します。

または、「既存のプロジェクトへの IAM アクセス許可の境界の追加」で説明しているように、プロジェクトにアクセス許可の境界を追加して、Lambda 関数のカスタムロールを使用できます。

GitHub リポジトリの接続を作成できません

問題:

GitHub リポジトリへの接続は AWS Connector for GitHub を使用するため、接続を作成するには、リポジトリへの組織所有者のアクセス許可または管理者アクセス許可が必要です。

解決方法: GitHub リポジトリのアクセス許可レベルの詳細については、https://docs.github.com/en/free-pro-team@latest/github/setting-up-and-managing-organizations-and-teams/permission-levels-for-an-organization を参照してください。

AWS CodeStar ユーザーガイドリリースノート

次の表に、 AWS CodeStar ユーザーガイドの各リリースにおける重要な変更点を示します。このドキュメントの更新に関する通知を受け取るには、RSS フィードにサブスクライブできます。

変更	説明	日付
アクセスポリシーの更新	AWS CodeStar アクセスロールポリシーが更新されました。ポリシーの結果は同じですが、CloudFormation には DescribeStacks に加えて ListStacks が必要です。これはすでに必須になっています。更新されたポリシーを確認するには、「AWSCodeStarServiceRole ポリシー」を参照してください。	2023 年 3 月 24 日
[Service role policy updates] (サービスロールポリシーの更新)	AWS CodeStar サービスロールポリシーが更新されました。更新されたポリシーを参照するには、[AWSCodeStarServiceRolePolicy] (AWSCodeStar サービスロールポリシー) を参照してください。	2021 年 9 月 23 日
GitHub ソースリポジトリを持つプロジェクト用に接続リソースを使用する	コンソールを使用して GitHub リポジトリ AWS CodeStar でにプロジェクトを作成する場合、接続リソースを使用して GitHub アクションを管理します。接続は GitHub Apps を使用します。以前の GitHub 認可では OAuth を使用していました。GitHub への接続を使用	2021 年 4 月 27 日

	するプロジェクトを作成する方法を示すチュートリアルについては、[Tutorial: Create a Project with a GitHub Source Repository] (チュートリアル: GitHub ソースリポジトリを使用してプロジェクトを作成する) を参照してください。このチュートリアルでは、プロジェクトソースリポジトリのプルリクエストを作成、レビュー、マージする方法についても説明します。	
AWS CodeStar が米国西部 (北カリフォルニア) リージョン AWS Cloud9 でサポート	AWS CodeStar は、米国西部 (北カリフォルニア) リージョン AWS Cloud9 での の使用をサポートするようになりました。詳細については、[Setting up Cloud9] (Cloud9 の設定) を参照してください。	2021 年 2 月 16 日
新しいコンソールエクスペリエンスを反映するようにドキュメントを更新する	2020 年 8 月 12 日、 AWS CodeStar サービスは AWS コンソールの新しいユーザーエクスペリエンスに移行しました。新しいコンソールエクスペリエンスに合わせてユーザーガイドが更新されました。	2020 年 8 月 12 日

AWS CodeStar プロジェクトは AWS CodeStar CLI で作成できます	AWS CodeStar プロジェクトは CLI コマンドを使用して作成できます。 は、ソースコードと指定したツールチェーンテンプレートを使用してプロジェクトとインフラストラクチャ AWS CodeStar を作成します。「Create a Project in AWS CodeStar (AWS CLI)」を参照してください。	2018 年 10 月 24 日
すべての AWS CodeStar プロジェクトテンプレートにインフラストラクチャ更新用の CloudFormation ファイルが含まれるようになりました	AWS CodeStar は と連携 CloudFormation し、コードを使用してクラウドでサポートサービスやサーバー、またはサーバーレスプラットフォームを作成できます。CloudFormation ファイルは、すべての AWS CodeStar プロジェクトテンプレートタイプ (Lambda、EC2、または Elastic Beanstalk コンピューティングプラットフォームでテンプレート) で使用できるようになりました。ファイルは、ソースリポジトリの `template.yml` に保存されています。ファイルを表示および変更して、プロジェクトにリソースを追加できます。[Project Templates] (プロジェクトテンプレート) を参照してください。	2018 年 8 月 3 日

AWS CodeStar ユーザーガイドの更新通知が RSS から利用可能に	AWS CodeStar ユーザーガイドの HTML バージョンでは、ドキュメントの更新リリースノートページに記載されている更新の RSS フィードがサポートされるようになりました。RSS フィードには、2018 年 6 月 30 日以降に行われた更新が含まれています。以前に発表された更新は、「ドキュメントの更新のリリースノート」ページで引き続き利用できます。このフィードをサブスクライブするには、トップメニューパネルの RSS ボタンを使用します。	2018 年 6 月 30 日

次の表は、2018 年 6 月 30 日以前の AWS CodeStar ユーザーガイドの各リリースにおける重要な変更点を示しています。

変更	説明	変更日
AWS CodeStar ユーザーガイドが GitHub で利用可能になりました	このガイドが GitHub で利用可能になりました。GitHub を使用して、フィードバックの送信およびこのガイドの内容に対する変更リクエストの送信もできます。詳細については、ガイドのナビゲーションバーの [Edit on GitHub] (GitHub で編集) アイコンを選択するか、GitHub ウェブサイトで awsdocs/aws-codestar-user-guide リポジトリを参照してください。	2018 年 2 月 22 日
AWS CodeStar がアジアパシフィック (ソウル) で利用可能に	AWS CodeStar がアジアパシフィック (ソウル) リージョンで利用可能になりました。詳細については、「Amazon Web Services 全般のリファレンス」の「AWS CodeStar」を参照してください。	2018 年 2 月 14 日

変更	説明	変更日
AWS CodeStar がアジアパシフィック (東京) およびカナダ (中部) で利用可能に	AWS CodeStar が、アジアパシフィック (東京) およびカナダ (中部) リージョンで利用可能になりました。詳細については、「Amazon Web Services 全般のリファレンス」の「AWS CodeStar」を参照してください。	2017 年 12 月 20 日
AWS CodeStar がをサポートするようになりました AWS Cloud9	AWS CodeStar では AWS Cloud9、ウェブブラウザベースのオンライン IDE である を使用してプロジェクトコードを操作することができるようになりました。詳細については、「AWS Cloud9 で を使用する AWS CodeStar」を参照してください。 サポートされている AWS リージョンのリストについては、 AWS Cloud9の「」を参照してくださいAmazon Web Services 全般のリファレンス。	2017 年 11 月 30 日
AWS CodeStar が GitHub をサポートするようになりました	AWS CodeStar で GitHub へのプロジェクトコードの保存がサポートされるようになりました。詳細については、[Create a Project] (プロジェクトの作成) を参照してください。	2017 年 10 月 12 日
AWS CodeStar が米国西部 (北カリフォルニア) および欧州 (ロンドン) で利用可能に	AWS CodeStar が米国西部 (北カリフォルニア) および欧州 (ロンドン) リージョンで利用可能になりました。詳細については、「Amazon Web Services 全般のリファレンス」の「AWS CodeStar」を参照してください。	2017 年 8 月 17 日
AWS CodeStar アジアパシフィック (シドニー) 、アジアパシフィック (シンガポール) 、欧州 (フランクフルト) で利用可能に	AWS CodeStar が、アジアパシフィック (シドニー) 、アジアパシフィック (シンガポール) 、欧州 (フランクフルト) の各リージョンで利用可能になりました。詳細については、「Amazon Web Services 全般のリファレンス」の「AWS CodeStar」を参照してください。	2017 年 7 月 25 日

変更	説明	変更日
AWS CloudTrail がをサポートするようになりました AWS CodeStar	AWS CodeStar は CloudTrail と統合されるようになりました。CloudTrail は、 AWS アカウント AWS CodeStar でによって行われた、または に代わって行われた API コールをキャプチャし、指定した Amazon S3 バケットに口グファイルを配信するサービスです。詳細については、「を使用した AWS CodeStar API コールの口グ記録 AWS CloudTrail」を参照してください。	2017 年 6 月 14 日
初回リリース	これは AWS CodeStar ユーザーガイドの最初のリリースです。	2017 年 4 月 19 日

AWS 用語集

最新の AWS 用語については、 AWS の用語集 リファレンスのAWS 用語集を参照してください。