ユーザーガイド

デベロッパーツールコンソール

デベロッパーツールコンソール: ユーザーガイド

Table of Contents

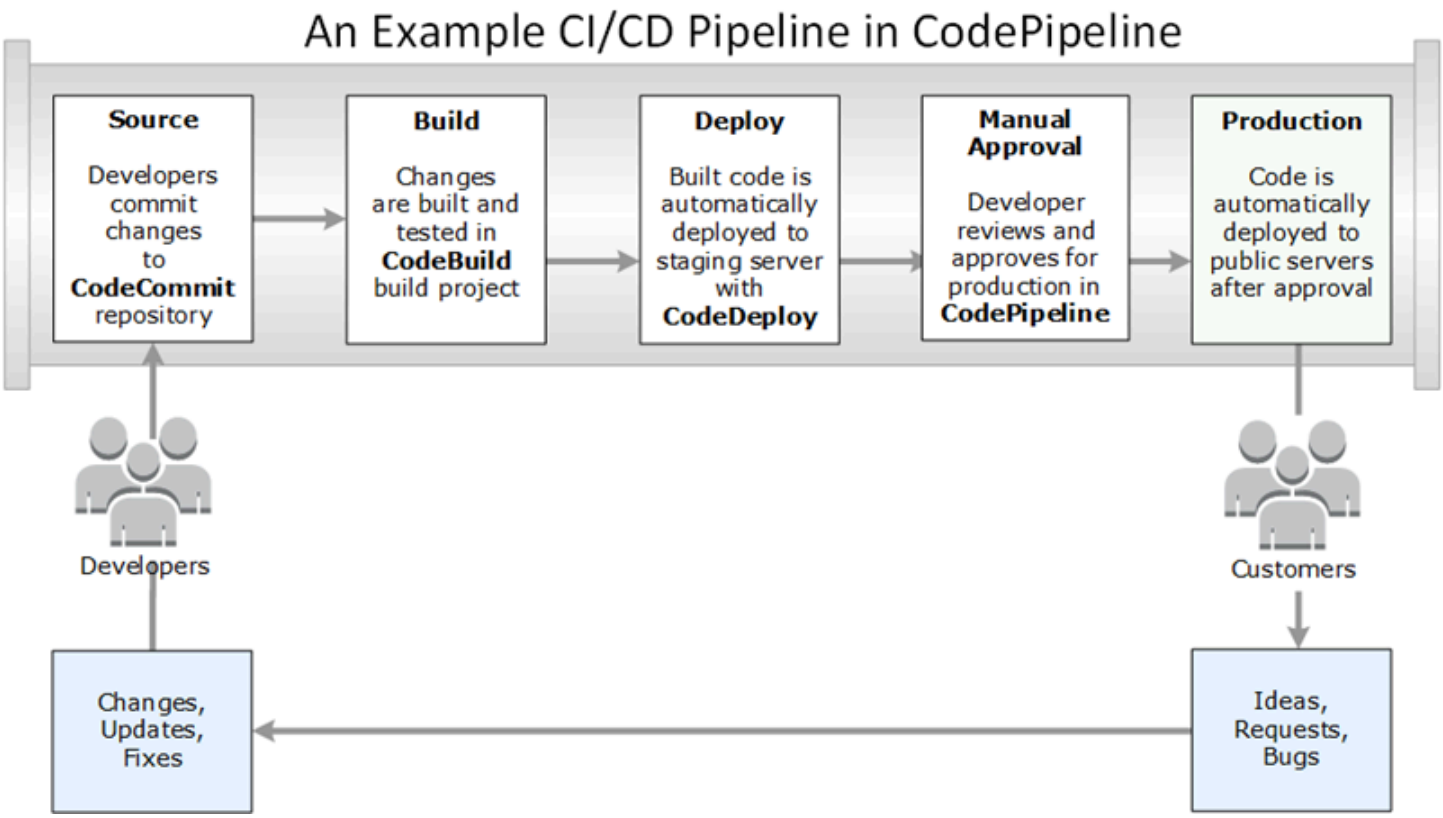
デベロッパーツールコンソールとは

デベロッパーツールコンソールには、ソフトウェアを開発するために個別にまたはまとめて使用できる、一連のサービスと機能があります。デベロッパーツールは、ソフトウェアを安全に保存、ビルド、テスト、およびデプロイするのに役立ちます。これらのツールは、個別にまたはまとめて使用し、DevOps、継続的インテグレーション、継続的デリバリー (CI/CD) をサポートします。

デベロッパーツールコンソールには、以下のサービスが含まれます。

- AWS CodeCommit は、プライベートの Git リポジトリをホストする、完全に管理されたソースコントロールサービスです。リポジトリを使用することで、アセット (ドキュメント、ソースコード、バイナリファイルなど) を AWS クラウドに非公開で保存および管理することができます。リポジトリには、最初のコミットから最新の変更までのプロジェクト履歴が保存されます。コードにコメントし、プルリクエストを作成して、コードの品質を確保することで、リポジトリ内のコードで共同で作業できます。
- AWS CodeBuild は完全マネージド型の構築サービスです。ソースコードのコンパイル、ユニットテストの実行、すぐにデプロイできるアーティファクトの生成を行います。Apache Maven、Gradle などの一般的なプログラミング言語とビルドツール用のパッケージ済みのビルド環境を提供します。ビルド環境をカスタマイズして、CodeBuild で独自のビルドツールを使用することもできます。
- AWS CodeDeploy は、Amazon EC2 やオンプレミスサーバーなどのコンピューティングサービスへのソフトウェアデプロイを自動化するフルマネージド AWS Lambdaデプロイサービスです。これにより、新しい機能を迅速にリリースし、アプリケーションのデプロイ中のダウンタイムを回避し、アプリケーションの更新に伴う複雑さを処理できます。
- AWS CodePipeline は、ソフトウェアをリリースするために必要な手順のモデル化、可視化、および自動化に使用できる継続的な統合および継続的な配信サービスです。ソフトウェアリリースプロセスのさまざまなステージを素早くモデル化して設定できます。お客様は、お客様が定義するリリースプロセスモデルに基づいて、コードの変更があるたびに、コードのビルド、テスト、デプロイを実施できます。

ここでは、 デベロッパーツールコンソールのサービスを一緒に使用して、ソフトウェアの開発を支援する方法の例を示します。



この例では、開発者が CodeCommit でリポジトリを作成し、それを使用してコードを開発して、共同作業します。CodeBuild でビルドプロジェクトを作成してコードをビルドおよびテストし、CodeDeploy を使用してテスト環境と実稼働環境にコードをデプロイします。すばやい反復処理が必要なため、CodePipeline でパイプラインを作成し、CodeCommit のリポジトリ内の変更を検出します。これらの変更がビルドされ、テストが実行され、正常にビルドされ、テストされたコードがテストサーバーにデプロイされます。チームは、テストステージをパイプラインに追加して、統合テストや負荷テストなど、ステージングサーバーでさらに多くのテストを実行します。これらのテストが正常に完了すると、チームメンバーは結果をレビューし、問題がない場合、本番用の変更を手動で承認します。CodePipeline は、テストされ承認されたコードを本番稼働用インスタンスにデプロイします。

これは、デベロッパーツールコンソールで提供されている 1 つまたは複数のサービスを使用してソフトウェアを開発する方法を示す簡単な例の 1 つです。各サービスは、ニーズに合わせてカスタマイズできます。では、他の製品やサービスと多くの統合が提供されています。また、他のサードパーティー製ツール AWS とも統合されています。詳細については、以下の各トピックを参照してください。

- CodeCommit: 製品とサービスの統合
- CodeBuild:Jenkins と連携した CodeBuild を使用する

- CodeDeploy: 製品およびサービスの統合
- CodePipeline:製品およびサービスの統合

を初めてお使いになる方向けの情報

デベロッパーツールコンソールで利用可能なサービスを初めて使用する場合は、まず以下のトピックを読むことをお勧めします。

- CodeCommit の開始方法
- CodeBuild の開始方法、概念
- https://docs.aws.amazon.com/codedeploy/latest/userguide/getting-started-codedeploy.html CodeDeploy の使用開始、プライマリコンポーネント
- CodePipeline の使用開始、概念

デベロッパーツールコンソールの機能

デベロッパーツールコンソールには、以下の機能も含まれます。

- デベロッパーツールコンソールには、、 AWS CodeBuild AWS CodeCommit AWS CodeDeploy、および のイベントをサブスクライブするために使用できる通知マネージャー機能が含まれています AWS CodePipeline。この機能には独自の API である AWS CodeStar Notifications があります。通知機能を使用して、のユーザーに対して、作業に最も重要なレポジトリ、ビルドプロジェクト、デプロイアプリケーション、パイプラインのイベントについてすばやく通知できます。通知マネージャーは、リポジトリ、ビルド、デプロイ、またはパイプラインで発生するイベントをユーザーに認識させ、変更の承認やエラーの修正などのアクションをすばやく実行できるようにします。詳細については、通知とは何ですか?を参照してください。
- デベロッパーツールコンソールには、 AWS リソースをサードパーティーのソースコードプロバイダーに関連付けるための接続機能も含まれています。この機能には独自の API、 AWS CodeConnections があります。接続機能を使用して、サードパーティープロバイダーとの認可された接続を設定し、その接続リソースを他の AWS のサービスで使用できます。詳細については、接続とは? を参照してください。

通知とは何ですか?

デベロッパーツールコンソールの通知機能は、 AWS CodeBuildおよび のイベントをサブスクライブするための通知マネージャーです AWS CodeCommit AWS CodeDeploy AWS CodePipeline。独自の API、 AWS CodeStar Notifications があります。通知機能を使用して、のユーザーに対して、作業に最も重要なレポジトリ、ビルドプロジェクト、デプロイアプリケーション、パイプラインのイベントについてすばやく通知できます。通知マネージャーは、リポジトリ、ビルド、デプロイ、またはパイプラインで発生するイベントをユーザーに認識させ、変更の承認やエラーの修正などのアクションをすばやく実行できるようにします。

通知でどのようなことができますか?

通知機能を使用して通知ルールを作成および管理することで、リソースに対する以下のような重要な変更をユーザーに通知できます。

- CodeBuild のビルドプロジェクトにおけるビルドの成功と失敗。
- CodeDeploy アプリケーションのデプロイの成功と失敗。
- CodeCommit リポジトリ内のプルリクエスト (コードに対するコメントを含む) の作成と更新 。
- CodePipeline での手動による承認のステータスとパイプラインの実行。

通知は、Amazon SNS トピックにサブスクライブしているユーザーの E メールアドレスに配信されるように設定できます。また、この機能を AWS Chatbot と統合し、Slack チャンネル、Microsoft Teams チャネル、または Amazon Chime チャットルームに通知を配信することもできます。

通知はどのような仕組みで機能しますか?

リポジトリ、ビルドプロジェクト、アプリケーション、またはパイプラインなど、サポートされているリソースに対する通知ルールを設定すると、通知機能は指定されたイベントをモニタリングする Amazon EventBridge ルールを作成します。このタイプのイベントが発生すると、通知ルールはそのルールのターゲットとして指定された Amazon SNS トピックに通知を送信します。これらのターゲットの受信者は、該当するイベントに関する通知を受け取ります。

通知の使用を開始する方法

使用を開始するには、次のいくつかのトピックが役立ちます。

- 通知の概念について説明します。

- 通知の操作を開始するために必要なリソースを設定します。
- 最初の通知ルールを開始し、最初の通知を受け取ります。

通知の概念

概念と用語を理解すれば、通知の設定と使用が容易になります。ここでは、通知を使用する際に知っておかなければならないいくつかの概念を次に示します。

トピック

- 通知
- 通知ルール
- Events
- 詳細タイプ
- ターゲット
- 通知と AWS CodeStar 通知
- リポジトリでの通知ルールのイベント
- ビルドプロジェクトでの通知ルールのイベント
- デプロイアプリケーションでの通知ルールのイベント
- パイプラインでの通知ルールのイベント

通知

通知とは、お客様と開発者が使用するリソースで発生するイベントに関する情報を示すメッセージです。ビルドプロジェクト、リポジトリ、デプロイアプリケーション、パイプラインなどのリソースのユーザーに対して、作成した通知ルールに従って、指定したイベントタイプに関する E メールを送信するように通知を設定できます。

の通知には、セッションタグを使用して、表示名や E メールアドレスなどのユーザー ID 情報を含める AWS CodeCommit ことができます。CodeCommit はセッションタグの使用をサポートしています。セッションタグは、IAM ロールを引き受けるとき、一時的な認証情報を使用するとき、または AWS Security Token Service () でユーザーをフェデレーションするときに渡すキーと値のペアの属性ですAWS STS。タグを IAM ユーザーに関連付けることもできます。CodeCommit は、`displayName` と `emailAddress` のタグが存在する場合、それらの値を通知コンテンツに含めます。詳細については、「CodeCommit で ID 情報を提供するためのタグの使用」を参照してください。

> **Important**
>
> 通知には、ビルドのステータス、デプロイのステータス、コメントのあるコード行、パイプラインの承認など、プロジェクト固有の情報が含まれます。通知の内容は、新機能が追加されると変更されることがあります。セキュリティのベストプラクティスとして、通知ルールのターゲットと Amazon SNS トピックのサブスクライバーを定期的に確認する必要があります。詳細については、「通知の内容とセキュリティについて」を参照してください。

通知ルール

通知ルールは、通知が送信されるタイミングと場所を指定するために作成する AWS リソースです。通知ルールでは、以下を定義します。

- 通知の作成条件。これらの条件は、選択したイベントに基づきます。イベントはリソースタイプに固有です。サポートされているリソースタイプには AWS CodeBuild、 のビルドプロジェクト、 のデプロイアプリケーション AWS CodeDeploy、 のパイプライン AWS CodePipeline、 のリポジトリなどがあります AWS CodeCommit。
- 通知の送信先のターゲット。通知ルールには最大 10 個のターゲットを指定できます。

通知ルールの送信先は、個別のビルドプロジェクト、デプロイアプリケーション、パイプライン、およびリポジトリです。通知ルールには、ユーザー定義のフレンドリ名と Amazon リソースネーム (ARN) の両方があります。通知ルールは、リソースが存在するのと同じ AWS リージョンで作成する必要があります。例えば、ビルドプロジェクトが 米国東部 (オハイオ) リージョンにある場合、通知ルールも 米国東部 (オハイオ) リージョンで作成する必要があります。

1 つのリソースに対して最大 10 個の通知ルールを定義できます。

Events

イベントとは、モニタリングするリソースの状態の変化です。各リソースには、選択できるイベントタイプのリストがあります。リソースに通知ルールを設定する際に、発生したときに通知が送信されるイベントを指定します。例えば、CodeCommit でリポジトリの通知を設定し、[Pull request] (プルリクエスト)と [Branches and tags] (ブランチとタグ) の両方で[Created] (作成済み) を選択した場合、そのリポジトリ内のユーザーがプルリクエスト、ブランチ、または Git タグを作成するたびに通知が送信されます。

詳細タイプ

通知ルールを作成するとき、通知に含まれる詳細レベルまたは詳細タイプ ([フル] または [ベーシック]) を選択できます。[フル] 設定 (デフォルト) では、通知にあるイベントについて入手可能な情報 (特定のイベントについてサービスから提供される拡張情報も含む) のすべてが含まれます。[ベーシック] 設定では、入手可能な情報のサブセットのみが含まれます。

以下の表では、特定のイベントタイプについて入手可能な拡張情報を一覧表示し、詳細タイプ間の違いについて説明します。

サービス	イベント	フルに含まれる	ベーシックには含まれない
CodeCommit	コミットに関するコメント プルリクエストに関するコメント	返信やコメントスレッドなど、すべてのイベントの詳細とコメントの内容。コメントが作成された行番号とコード行も含まれます。	コメントの内容、行番号、コード行、コメントスレッド。
CodeCommit	プルリクエストが作成された	すべてのイベントの詳細、および送信先ブランチに関連するプルリクエストで追加、変更、または削除されたファイルの数。	プルリクエストの送信元ブランチによって追加、変更、または削除されたファイルのリストや詳細。
CodePipeline	手動承認を求められた	すべてのイベントの詳細とカスタムデータ (設定されている場合)。通知には、パイプラインで求められる承認へのリンクも含まれます。	カスタムデータまたはリンク。

サービス	イベント	フルに含まれる	ベーシックには含まれない
CodePipeline	アクションの実行に失敗した パイプラインの実行に失敗した ステージの実行に失敗した	すべてのイベントの詳細と失敗のエラーメッセージの内容。	エラーメッセージの内容。

ターゲット

ターゲットとは、通知ルールからの通知が届く場所です。許可されるターゲットタイプは、Slack または Microsoft Teams チャネル用に設定された Amazon SNS トピックと AWS Chatbot クライアントです。ターゲットにサブスクライブしているすべてのユーザーに、通知ルールで指定したイベントに関する通知が送信されます。

通知の到達範囲を拡張する場合は、通知が Amazon Chime チャットルームに送信されるように、通知と AWS Chatbot の統合を手動で設定できます。その後、その AWS Chatbot クライアント用に設定された Amazon SNS トピックを通知ルールのターゲットとして選択できます。詳細については、「Chatbot および Amazon Chime AWS と通知を統合するには」を参照してください。

AWS Chatbot クライアントをターゲットとして使用する場合は、まず AWS Chatbot でそのクライアントを作成する必要があります。 AWS Chatbot クライアントを通知ルールのターゲットとして選択すると、通知を Slack または Microsoft Teams チャネルに送信するために必要なすべてのポリシーを持つ Amazon SNS トピックがその AWS Chatbot クライアント用に設定されます。 AWS Chatbot クライアントの既存の Amazon SNS トピックを設定する必要はありません。

通知ルールの作成の一環として、Amazon SNS トピックをターゲットとして作成を選択できます (推奨)。通知ルールと同じ AWS リージョンにある既存の Amazon SNS トピックを選択することもできますが、必要なポリシーで設定する必要があります。ターゲットに使用する Amazon SNS トピックは、 AWS アカウントに存在する必要があります。また、通知ルールおよびルールが作成された AWS リソースと同じ AWS リージョンに存在する必要があります。

例えば、米国東部 (オハイオ) リージョンでリポジトリの通知ルールを作成した場合、Amazon SNS トピックもそのリージョンに存在する必要があります。通知ルールの作成の一部として Amazon

SNS トピックを作成すると、トピックへのイベントの公開を許可するために必要なポリシーによりトピックが設定されます。これは、ターゲットと通知ルールを操作するのに最適な方法です。既存のトピックを使用するか、手動でトピックを作成する場合は、ユーザーが通知を受け取る前に、必要なアクセス許可でトピックを設定する必要があります。詳細については、「通知用に Amazon SNS トピックを設定する」を参照してください。

> **Note**
>
> 新しいトピックを作成する代わりに既存の Amazon SNS トピックを使用する場合は、[Targets (ターゲット)] でその ARN を選択します。トピックに適切なアクセスポリシーがあり、リソースに関する情報を表示できるユーザーのみがサブスクライバーリストに含まれていることを確認します。Amazon SNS トピックが 2019 年 11 月 5 日より前に CodeCommit 通知に使用されたトピックである場合、CodeStar Notifications に必要な AWS CodeStar CodeCommit への発行を許可するポリシーが含まれます。これらのトピックの使用は非推奨です。そのエクスペリエンス用に作成されたポリシーを使用する場合は、既存のポリシーに加えて、 AWS CodeStar Notifications に必要なポリシーを追加する必要があります。詳細については、「通知用に Amazon SNS トピックを設定する」および「通知の内容とセキュリティについて」を参照してください。

通知と AWS CodeStar 通知

デベロッパーツールコンソールの機能では、通知には独自の API、 AWS CodeStar Notifications があります。また、独自の AWS リソースタイプ (通知ルール) 、アクセス許可、イベントもあります。通知ルールのイベントはログインした AWS CloudTrailです。API アクションは、 IAM ポリシーを通じて許可または拒否できます。

リポジトリでの通知ルールのイベント

Category	Events	イベント ID

コメント	コミット時
	
	プルリクエスト時
		`codecommit-repository-comments-on-commits`
		
		`codecommit-repository-comments-on-pull-requests`

Category	Events	イベント ID
承認	ステータス変更 ルールの上書き	codecommit-repository-approvals-status-changed codecommit-repository-approvals-rule-override
プルリクエスト	作成 ソース更新 ステータス変更 マージ	codecommit-repository-pull-request-created codecommit-repository-pull-request-source-updated codecommit-repository-pull-request-status-changed codecommit-repository-pull-request-merged
ブランチとタグ	作成 [Deleted] (削除済み) 更新	codecommit-repository-branches-and-tags-created codecommit-repository-branches-and-tags-deleted codecommit-repository-branches-and-tags-updated

ビルドプロジェクトでの通知ルールのイベント

Category	Events	イベント ID
ビルド状態	失敗 成功 進行中 停止	codebuild-project-build-state-failed codebuild-project-build-state-succeeded codebuild-project-build-state-in-progress codebuild-project-build-state-stopped
ビルドフェーズ	失敗 Success	codebuild-project-build-phase-failure codebuild-project-build-phase-success

デプロイアプリケーションでの通知ルールのイベント

Category	Events	イベント ID
デプロイメント	失敗 成功 起動済み	codedeploy-application-deployment-failed codedeploy-application-deployment-succeeded codedeploy-application-deployment-started

パイプラインでの通知ルールのイベント

Category	Events	イベント ID
アクションの実行	成功 失敗 キャンセル 起動済み	codepipeline-pipeline-action-execution-succeeded codepipeline-pipeline-action-execution-failed codepipeline-pipeline-action-execution-canceled codepipeline-pipeline-action-execution-started
ステージの実行	起動済み 成功 再開 Canceled 失敗	codepipeline-pipeline-stage-execution-started codepipeline-pipeline-stage-execution-succeeded codepipeline-pipeline-stage-execution-resumed codepipeline-pipeline-stage-execution-canceled codepipeline-pipeline-stage-execution-failed
パイプラインの実行	失敗 キャンセル 起動済み 再開 成功	codepipeline-pipeline-pipeline-execution-failed codepipeline-pipeline-pipeline-execution-canceled codepipeline-pipeline-pipeline-execution-started

Category	Events	イベント ID
	優先	codepipeline-pipeline-pipeline-execution-resumed codepipeline-pipeline-pipeline-execution-succeeded codepipeline-pipeline-pipeline-execution-superseded
手動の承認	失敗 必要 成功	codepipeline-pipeline-manual-approval-failed codepipeline-pipeline-manual-approval-needed codepipeline-pipeline-manual-approval-succeeded

セットアップ

IAM ユーザーまたはロールの管理ポリシーがある場合 AWS CodeBuild AWS CodeCommit AWS CodeDeploy、または IAM ユーザーまたはロール AWS CodePipeline に適用されている場合は、ポリシーによって提供されるロールとアクセス許可の制限内で通知を操作するために必要なアクセス許可があります。例えば、AWSCodeBuildAdminAccess、AWSCodeCommitFullAccess、AWSCodeDeployFullAccess、または AWSCodePipeline_FullAccess 管理ポリシーが適用されたユーザーには、通知に対する完全な管理アクセスがあります。

詳細とポリシーの例については、「アイデンティティベースのポリシー」を参照してください。

これらのポリシーのいずれかを IAM ユーザーまたはロールに適用し、CodeBuild のビルドプロジェクト、CodeCommit のリポジトリ、CodeDeploy のデプロイアプリケーション、または CodePipeline のパイプラインに適用している場合、最初の通知ルールを作成する準備ができています。「通知の使用開始」に進みます。そうでない場合は、以下のトピックを参照してください。

- CodeBuild: CodeBuild の開始方法
- CodeCommit: CodeCommit の開始方法

- CodeDeploy: チュートリアル
- CodePipeline: CodePipeline の使用開始

IAM ユーザー、グループ、またはロールの通知の管理アクセス許可を自分で管理する場合は、このトピックの手順に従って、サービスを使用するために必要なアクセス許可とリソースを設定します。

通知専用のトピックを作成する代わりに、以前に作成した Amazon SNS トピックを通知に使用する場合は、そのトピックへのイベントの発行を許可するポリシーを適用して、通知ルールのターゲットとして使用する Amazon SNS トピックを設定する必要があります。

> **Note**
>
> 以下の手順を実行するには、管理者権限を持つアカウントで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 管理者ユーザーおよびユーザーグループの作成」を参照してください。

トピック

- 通知への管理アクセスのためのポリシーの作成と適用
- 通知用に Amazon SNS トピックを設定する
- ターゲットである Amazon SNS トピックへのユーザーのサブスクライブ

通知への管理アクセスのためのポリシーの作成と適用

通知を管理するには、IAM ユーザーでサインインするか、通知を作成するサービスおよびサービス (AWS CodeBuild AWS CodeCommit、 AWS CodeDeploy、または AWS CodePipeline) へのアクセス許可を持つロールを使用します。独自のポリシーを作成し、ユーザーまたはグループに適用することもできます。

次の手順では、通知を管理し、IAM ユーザーを追加するアクセス許可を持つ IAM グループを設定する方法を示します。グループをセットアップしない場合は、このポリシーを IAM ユーザーに直接適用するか、ユーザーが引き受けることができる IAM ロールに直接適用できます。ポリシーの範囲に応じて、ポリシーに適切な通知機能へのアクセスが含まれる、CodeBuild、CodeCommit、CodeDeploy、または CodePipeline の管理ポリシーを使用することもできます。

以下のポリシーに、このポリシーの名前 (例: AWSCodeStarNotificationsFullAccess) と説明 (省略可能) を入力します。この説明は、ポリシーの目的を思い出すのに役立ちます (例: **This policy provides full access to AWS CodeStar Notifications.**)。

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/ 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。

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

6. 次へ を選択します。

> **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、[ビジュアル] 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ビジュアル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. ポリシーを作成 をクリックして、新しいポリシーを保存します。

通知用に Amazon SNS トピックを設定する

通知を設定する最も簡単な方法は、通知ルールを作成するときに Amazon SNS トピックを作成することです。以下の要件を満たしている場合は、既存の Amazon SNS トピックを使用できます。

- これは、通知ルールを作成するリソース (ビルドプロジェクト、デプロイアプリケーション、リポジトリ、またはパイプライン) AWS リージョン と同じ に作成されました。
- 2019 年 11 月 5 日より前の CodeCommit の通知を送信するためには使用されていません。使用している場合は、その機能を有効にしたポリシーステートメントが含まれます。このトピックを使用することもできますが、手順で指定されているように、追加のポリシーを追加する必要があります。2019 年 11 月 5 日より前に通知用に 1 つ以上のリポジトリーが設定されている場合は、既存のポリシーステートメントを削除しないでください。
- これには、 AWS CodeStar Notifications がトピックに通知を発行することを許可するポリシーがあります。

AWS CodeStar Notifications 通知ルールのターゲットとして使用するように Amazon SNS トピックを設定するには

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/sns/v3/home で Amazon SNS コンソールを開きます。
2. ナビゲーションバーで、[トピック] を選択し、設定するトピックを選択して、[編集] を選択します。

3. [アクセスポリシー]を展開し、アドバンストを選択します。
4. JSON エディタで、ポリシーに次のポリシーステートメントを追加します。トピック ARN、AWS リージョン AWS アカウント ID、トピック名を含めます。

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

このポリシーステートメントは、次のようになります。

```
{
  "Version": "2008-10-17",
  "Id": "__default_policy_ID",
  "Statement": [
    {
      "Sid": "__default_statement_ID",
      "Effect": "Allow",
      "Principal": {
        "AWS": "*"
      },
      "Action": [
        "SNS:GetTopicAttributes",
        "SNS:SetTopicAttributes",
        "SNS:AddPermission",
        "SNS:RemovePermission",
        "SNS:DeleteTopic",
        "SNS:Subscribe",
        "SNS:ListSubscriptionsByTopic",
        "SNS:Publish"
      ],
      "Resource": "arn:aws:sns:us-east-2:123456789012:codestar-notifications-
MyTopicForNotificationRules",
      "Condition": {
```

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

5. [Save changes] (変更の保存) をクリックします。
6. AWS KMS暗号化された Amazon SNS トピックを使用して通知を送信する場合は、次のステートメントを のポリシーに追加して、イベントソース (AWS CodeStar Notifications) と暗号化されたトピックとの互換性も有効にする必要があります AWS KMS key。 AWS リージョン (この例では us-east-2) を、キーが作成された AWS リージョン に置き換えます。

   JSON

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

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

詳細については、「保管時の暗号化」および「AWS KMSでのポリシー条件の使用」のAWS Key Management Service デベロッパーガイドを参照してください。

ターゲットである Amazon SNS トピックへのユーザーのサブスクライブ

ユーザーが通知を受信できるようにするには、通知ルールのターゲットである Amazon SNS トピックにサブスクライブする必要があります。ユーザーが E メールアドレスでサブスクライブしている場合、通知を受け取る前にサブスクリプションを確認する必要があります。Slack チャンネル、Microsoft Teams チャネル、または Amazon Chime チャットルームのユーザーに通知を送信するには、「通知と AWS Chatbot の統合を設定する」を参照してください。

通知に使用する Amazon SNS トピックにユーザーをサブスクライブするには

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/sns/v3/home で Amazon SNS コンソールを開きます。
2. ナビゲーションバーで、[トピック] を選択し、ユーザーをサブスクライブするトピックを選択します。
3. [サブスクリプション] で、[サブスクリプションの作成] を選択します。
4. [プロトコル] で、[E メール] を選択します。[エンドポイント] にメールアドレスを入力し、[サブスクリプションの作成] を選択します。

通知の使用開始

通知の使用を開始する最も簡単な方法は、ビルドプロジェクト、デプロイアプリケーション、パイプライン、またはリポジトリのいずれかに通知ルールを設定することです。

> **Note**
>
> 通知ルールを初めて作成すると、サービスにリンクされたロールがアカウントに作成されます。詳細については、「AWS CodeStar Notifications のサービスにリンクされたロールの使用」を参照してください。

トピック

前提条件

「セットアップ」のステップを完了します。通知ルールを作成するリソースも必要です。

- CodeBuild でビルドプロジェクトを作成するか、既存のプロジェクトを使用します。
- アプリケーションを作成するか、既存のデプロイアプリケーションを使用します。
- CodePipeline でパイプラインを作成するか、既存のパイプラインを使用します。
- AWS CodeCommit リポジトリを作成するか、既存のリポジトリを使用します。

リポジトリの通知ルールを作成する

通知ルールを作成して、重要なリポジトリイベントに関する通知を送信できます。以下のステップは、単一のリポジトリイベントに関する通知ルールを設定する方法を示しています。これらのステップは、 AWS アカウントにリポジトリが設定されていることを前提としています。

> **Important**
>
> 2019 年 11 月 5 日より前に CodeCommit で通知を設定した場合、それらの通知に使用される Amazon SNS トピックには、CodeStar Notifications に必要な AWS CodeStar CodeCommit への発行を許可するポリシーが含まれます。これらのトピックの使用は非推奨です。そのエクスペリエンス用に作成されたポリシーを使用する場合は、既存のポリシーに

加えて、 AWS CodeStar Notifications に必要なポリシーを追加する必要があります。詳細については、「通知用に Amazon SNS トピックを設定する」および「通知の内容とセキュリティについて」を参照してください。

1. https://console.aws.amazon.com/codecommit/ で CodeCommit コンソールを開きます。
2. リストからリポジトリを選択して開きます。
3. [Notify (通知)]、[Create notification rule (通知ルールの作成)] の順に選択します。[設定]、[通知]、[通知ルールの作成] の順に選択することもできます。
4. [通知名] に、ルールの名前を入力します。
5. Amazon EventBridge に提供された情報のみを通知に含める場合は、[Detail type (詳細タイプ)] で [Basic (基本)] を選択します。Amazon EventBridge に提供される情報に加えて、リソースサービスまたは通知マネージャから提供される場合がある情報も含める場合は、[Full] (完全) を選択します。

   詳細については、「通知の内容とセキュリティについて」を参照してください。
6. [Events that trigger notifications (通知をトリガーするイベント)] の [ブランチとタグ] で、[作成済み] を選択します。
7. [ターゲット] で、[SNS トピックの作成] を選択します。

> **Note**
>
> 通知ルールの作成の一環としてトピックを作成すると、CodeCommit にトピックへのイベントの発行を許可するポリシーが適用されます。通知ルール用に作成されたトピックを使用すると、このリポジトリに関する通知の受信を希望するユーザーのみをサブスクライブできます。

[codestar-notifications-] プレフィックスの後にトピックの名前を入力し、[送信] を選択します。

> **Note**
>
> 新しいトピックを作成する代わりに既存の Amazon SNS トピックを使用する場合は、[Targets (ターゲット)] でその ARN を選択します。トピックに適切なアクセスポリシーがあり、リソースに関する情報を表示できるユーザーのみがサブスクライバーリストに含まれていることを確認します。Amazon SNS トピックが 2019 年 11 月 5 日より前に

CodeCommit 通知に使用されたトピックである場合、CodeStar Notifications に必要な AWS CodeStar CodeCommit への発行を許可するポリシーが含まれます。これらのトピックの使用は非推奨です。その エクスペリエンス用に作成されたポリシーを使用する場合は、既存のポリシーに加えて、 AWS CodeStar Notifications に必要なポリシーを追加する必要があります。詳細については、「通知用に Amazon SNS トピックを設定する」および「通知の内容とセキュリティについて」を参照してください。

8. [送信] を選択し、通知ルールを確認します。
9. 自分のメールアドレスを作成した Amazon SNS トピックにサブスクライブします。詳細については、「通知に使用する Amazon SNS トピックにユーザーをサブスクライブするには」を参照してください。
10. リポジトリに移動し、デフォルトブランチからテストブランチを作成します。
11. ブランチを作成すると、通知ルールによって、そのイベントに関する情報を含む通知がすべてのトピックサブスクライバーに送信されます。

ビルドプロジェクトの通知ルールを作成する

通知ルールを作成して、ビルドプロジェクトでの重要なイベントに関する通知を送信できます。以下のステップは、単一のビルドプロジェクトイベントに関する通知ルールを設定する方法を示しています。これらのステップは、 AWS アカウントでビルドプロジェクトが設定されていることを前提としています。

1. CodeBuild コンソール (https://console.aws.amazon.com/codebuild/) を開きます。
2. リストからビルドプロジェクトを選択して開きます。
3. [Notify (通知)]、[Create notification rule (通知ルールの作成)] の順に選択します。[設定]、[通知ルールの作成] の順に選択することもできます。
4. [通知名] に、ルールの名前を入力します。
5. Amazon EventBridge に提供された情報のみを通知に含める場合は、[Detail type (詳細タイプ)] で [Basic (基本)] を選択します。Amazon EventBridge に提供される情報に加えて、リソースサービスまたは通知マネージャから提供される場合がある情報も含める場合は、[Full] (完全) を選択します。

   詳細については、「通知の内容とセキュリティについて」を参照してください。
6. [Events that trigger notifications (通知をトリガーするイベント)] の [ビルドフェーズ] で、[成功] を選択します。

7. [ターゲット] で、[SNS トピックの作成] を選択します。

> **Note**
>
> 通知ルールの作成の一環としてトピックを作成すると、CodeBuild にトピックへのイベントの発行を許可するポリシーが適用されます。通知ルール用に作成されたトピックを使用すると、このビルドプロジェクトに関する通知の受信を希望するユーザーのみをサブスクライブできます。

[codestar-notifications-] プレフィックスの後にトピックの名前を入力し、[送信] を選択します。

> **Note**
>
> 新しいトピックを作成する代わりに既存の Amazon SNS トピックを使用する場合は、[Targets (ターゲット)] でその ARN を選択します。トピックに適切なアクセスポリシーがあり、リソースに関する情報を表示できるユーザーのみがサブスクライバーリストに含まれていることを確認します。Amazon SNS トピックが 2019 年 11 月 5 日より前に CodeCommit 通知に使用されたトピックである場合、CodeStar Notifications に必要な AWS CodeStar CodeCommit への発行を許可するポリシーが含まれます。これらのトピックの使用は非推奨です。そのエクスペリエンス用に作成されたポリシーを使用する場合は、既存のポリシーに加えて、 AWS CodeStar Notifications に必要なポリシーを追加する必要があります。詳細については、「通知用に Amazon SNS トピックを設定する」および「通知の内容とセキュリティについて」を参照してください。

8. [送信] を選択し、通知ルールを確認します。
9. 自分のメールアドレスを作成した Amazon SNS トピックにサブスクライブします。詳細については、「通知に使用する Amazon SNS トピックにユーザーをサブスクライブするには」を参照してください。
10. ビルドプロジェクトに移動し、ビルドを開始します。
11. ビルドフェーズが正常に完了すると、通知ルールは、そのイベントに関する情報を含む通知をすべてのトピックサブスクライバーに送信します。

デプロイアプリケーションの通知ルールを作成する

通知ルールを作成して、デプロイアプリケーションでの重要なイベントに関する通知を送信できます。以下のステップは、単一のビルドプロジェクトイベントに関する通知ルールを設定する方法を示

しています。これらの手順は、 AWS アカウントにデプロイアプリケーションが設定されていることを前提としています。

1. CodeDeploy コンソールは次の URL で開きます。https://console.aws.amazon.com/codedeploy/
2. リストからアプリケーションを選択して開きます。
3. [Notify (通知)]、[Create notification rule (通知ルールの作成)] の順に選択します。[設定]、[通知ルールの作成] の順に選択することもできます。
4. [通知名] に、ルールの名前を入力します。
5. Amazon EventBridge に提供された情報のみを通知に含める場合は、[Detail type (詳細タイプ)] で [Basic (基本)] を選択します。Amazon EventBridge に提供される情報に加えて、リソースサービスまたは通知マネージャから提供される場合がある情報も含める場合は、[Full] (完全) を選択します。

   詳細については、「通知の内容とセキュリティについて」を参照してください。

6. [Events that trigger notifications (通知をトリガーするイベント)] の [デプロイ] で、[成功] を選択します。
7. [ターゲット] で、[SNS トピックの作成] を選択します。

> **Note**
>
> 通知ルールの作成の一環としてトピックを作成すると、CodeDeploy にトピックへのイベントの発行を許可するポリシーが適用されます。通知ルール用に作成されたトピックを使用すると、このデプロイアプリケーションに関する通知の受信を希望するユーザーのみをサブスクライブできます。

[codestar-notifications-] プレフィックスの後にトピックの名前を入力し、[送信] を選択します。

> **Note**
>
> 新しいトピックを作成する代わりに既存の Amazon SNS トピックを使用する場合は、[Targets (ターゲット)] でその ARN を選択します。トピックに適切なアクセスポリシーがあり、リソースに関する情報を表示できるユーザーのみがサブスクライバーリストに含まれていることを確認します。Amazon SNS トピックが 2019 年 11 月 5 日より前に CodeCommit 通知に使用されたトピックである場合、CodeStar Notifications に必要な AWS CodeStar CodeCommit への発行を許可するポリシーが含まれます。これらのト

ピックの使用は非推奨です。そのエクスペリエンス用に作成されたポリシーを使用する場合は、既存のポリシーに加えて、 AWS CodeStar Notifications に必要なポリシーを追加する必要があります。詳細については、「通知用に Amazon SNS トピックを設定する」および「通知の内容とセキュリティについて」を参照してください。

8. [送信] を選択し、通知ルールを確認します。
9. 自分のメールアドレスを作成した Amazon SNS トピックにサブスクライブします。詳細については、「通知に使用する Amazon SNS トピックにユーザーをサブスクライブするには」を参照してください。
10. デプロイアプリケーションに移動し、デプロイを開始します。
11. デプロイが成功すると、通知ルールによって、そのイベントに関する情報を含む通知がすべてのトピックサブスクライバーに送信されます。

パイプラインの通知ルールを作成する

通知ルールを作成して、パイプラインの重要なイベントに関する通知を送信できます。以下のステップは、単一のパイプラインイベントに関する通知ルールを設定する方法を示しています。これらのステップは、 AWS アカウントにパイプラインが設定されていることを前提としています。

1. CodePipeline コンソールは次の URL で開きます。https://console.aws.amazon.com/codesuite/codepipeline/home
2. リストからパイプラインを選択して開きます。
3. [Notify (通知)]、[Create notification rule (通知ルールの作成)] の順に選択します。[設定]、[通知ルールの作成] の順に選択することもできます。
4. [通知名] に、ルールの名前を入力します。
5. Amazon EventBridge に提供された情報のみを通知に含める場合は、[Detail type (詳細タイプ)] で [Basic (基本)] を選択します。Amazon EventBridge に提供される情報に加えて、リソースサービスまたは通知マネージャから提供される場合がある情報も含める場合は、[Full] (完全) を選択します。

   詳細については、「通知の内容とセキュリティについて」を参照してください。
6. [Events that trigger notifications (通知をトリガーするイベント)] の [アクションの実行] で、[開始済] を選択します。
7. [ターゲット] で、[SNS トピックの作成] を選択します。

> **Note**
>
> 通知ルールの作成の一環としてトピックを作成すると、CodePipeline にトピックへのイベントの発行を許可するポリシーが適用されます。通知ルール用に作成されたトピックを使用すると、このパイプラインに関する通知の受信を希望するユーザーのみをサブスクライブできます。

[codestar-notifications-] プレフィックスの後にトピックの名前を入力し、[送信] を選択します。

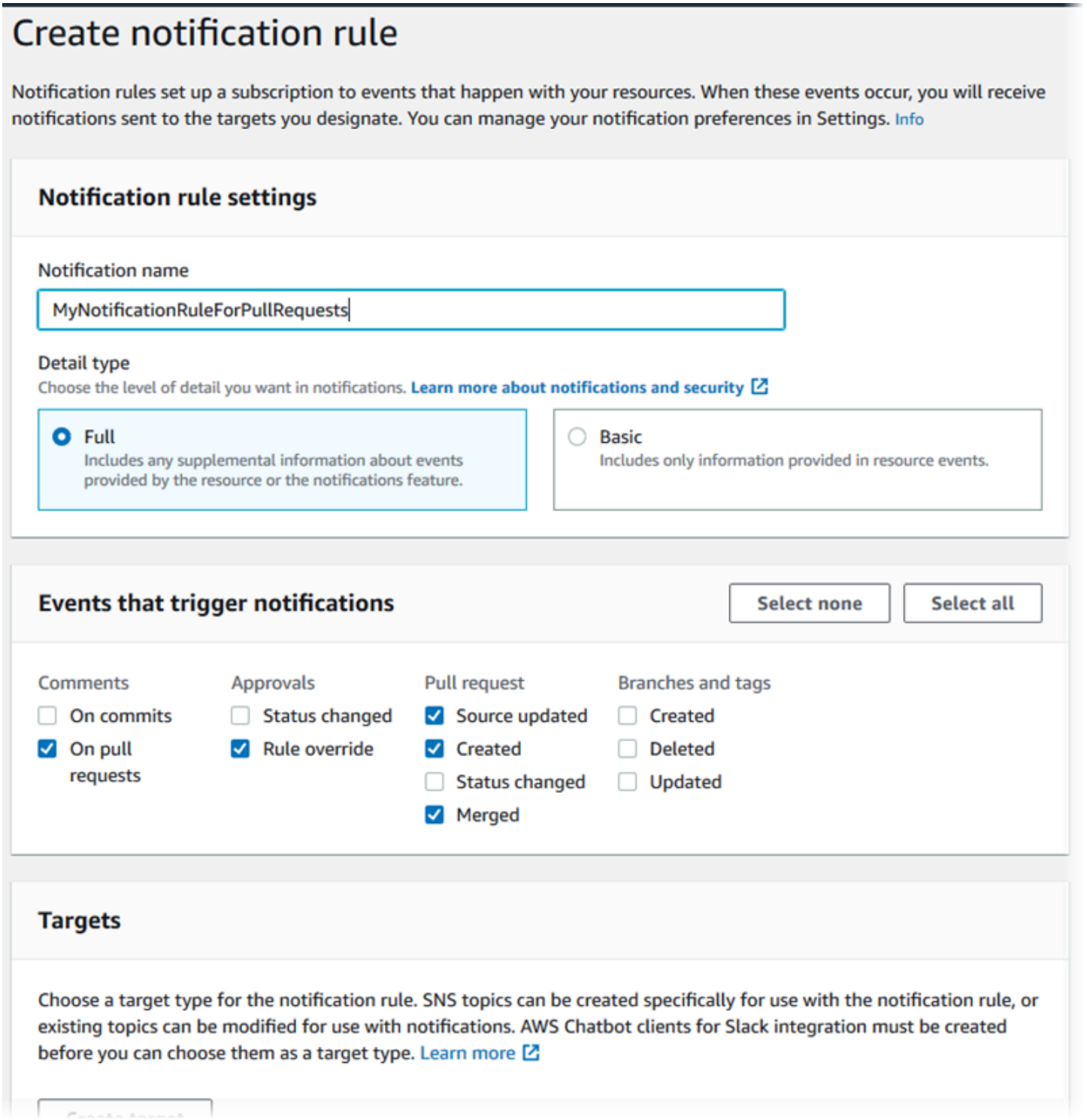
> **Note**
>
> 新しいトピックを作成する代わりに既存の Amazon SNS トピックを使用する場合は、[Targets (ターゲット)] でその ARN を選択します。トピックに適切なアクセスポリシーがあり、リソースに関する情報を表示できるユーザーのみがサブスクライバーリストに含まれていることを確認します。Amazon SNS トピックが 2019 年 11 月 5 日より前に CodeCommit 通知に使用されたトピックである場合、CodeStar Notifications に必要な AWS CodeStar CodeCommit への発行を許可するポリシーが含まれます。これらのトピックの使用は非推奨です。その エクスペリエンス用に作成されたポリシーを使用する場合は、既存のポリシーに加えて、 AWS CodeStar Notifications に必要なポリシーを追加する必要があります。詳細については、「通知用に Amazon SNS トピックを設定する」および「通知の内容とセキュリティについて」を参照してください。

8. [送信] を選択し、通知ルールを確認します。
9. 自分のメールアドレスを作成した Amazon SNS トピックにサブスクライブします。詳細については、「通知に使用する Amazon SNS トピックにユーザーをサブスクライブするには」を参照してください。
10. パイプラインに移動し、[Release change (変更のリリース)] を選択します。
11. アクションが開始されると、通知ルールによって、そのイベントに関する情報を含む通知がすべてのトピックサブスクライバーに送信されます。

通知ルールの使用

通知ルールでは、ユーザーに通知するイベントを設定し、これらの通知を受け取るターゲットを指定します。Amazon SNS を通じて、または Slack または Microsoft Teams チャネル用に設定された

AWS Chatbot クライアントを通じて、ユーザーに通知を直接送信できます。通知の到達範囲を拡張する場合は、通知が Amazon Chime チャットルームに送信されるように、通知と AWS Chatbot の統合を手動で設定できます。詳細については、「ターゲット」および「Chatbot および Amazon Chime AWS と通知を統合するには」を参照してください。



デベロッパーツールコンソールまたは を使用して AWS CLI 、通知ルールを作成および管理できます。

トピック

通知ルールの作成

デベロッパーツールコンソールまたは AWS CLI を使用して、通知ルールを作成できます。通知ルールの作成の一環として、通知ルールのターゲットとして使用する Amazon SNS トピックを作成できます。 AWS Chatbot クライアントをターゲットとして使用する場合は、ルールを作成する前にそのクライアントを作成する必要があります。詳細については、「Slack チャネルの AWS Chatbot クライアントを設定する」を参照してください。

通知ルールを作成するには (コンソール)

1. https://console.aws.amazon.com/codesuite/settings/notifications で AWS デベロッパーツールコンソールを開きます。
2. ナビゲーションバーを使用して、リソースに移動します。
   - CodeBuild では、[Build] (ビルド) 、[Build projects] (ビルドプロジェクト) の順に選択し、ビルドプロジェクトを選択します。
   - CodeCommit では、[Source] (ソース)、[Repositories] (リポジトリ) の順に選択し、リポジトリを選択します。
   - CodeDeploy では、[アプリケーション] を選択し、アプリケーションを選択します。
   - CodePipeline では、[Pipeline] (パイプライン) 、[Pipelines] (パイプライン) の順に選択し、パイプラインを選択します。
3. リソースページで、[Notify (通知)]、[Create notification rule (通知ルールの作成)] の順に選択します。リソースの [設定] ページの [通知] または [通知ルール] に移動し、[通知ルールの作成] を選択することもできます。
4. [通知名] に、ルールの名前を入力します。

5. Amazon EventBridge に提供された情報のみを通知に含める場合は、[Detail type (詳細タイプ)] で [Basic (基本)] を選択します。Amazon EventBridge に提供される情報に加えて、リソースサービスまたは通知マネージャから提供される場合がある情報も含める場合は、[Full] (完全) を選択します。

   詳細については、「通知の内容とセキュリティについて」を参照してください。

6. [Events that trigger notifications (通知をトリガーするイベント)] で、通知を送信するイベントを選択します。リソースのイベントタイプについては、以下を参照してください。

   - CodeBuild: ビルドプロジェクトでの通知ルールのイベント
   - CodeCommit: リポジトリでの通知ルールのイベント
   - CodeDeploy: デプロイアプリケーションでの通知ルールのイベント
   - CodePipeline: パイプラインでの通知ルールのイベント

7. [Targets (ターゲット)] で、次のいずれかの操作を行います。

   - 通知で使用するリソースを設定済みである場合は、[ターゲットタイプを選択] で、[AWS Chatbot (Slack)]、[AWS Chatbot (Microsoft Teams)]、または [SNS トピック] を選択します。ターゲットの選択で、クライアントの名前 (AWS Chatbot で設定された Slack または Microsoft Teams クライアントの場合) または Amazon SNS トピックの Amazon リソースネーム (ARN) (通知に必要なポリシーで既に設定された Amazon SNS トピックの場合) を選択します。
   - 通知で使用するリソースを設定していない場合は、[Create target]、[SNS topic] の順に選択します。codestar-notifications- の後にトピックの名前を指定し、[Create] を選択します。

> **Note**
>
> - 通知ルールの作成の一環として Amazon SNS トピックを作成すると、トピックへのイベント発行を通知機能に許可するポリシーが適用されます。通知ルール用に作成したトピックを使用すると、このリソースに関する通知を受信するユーザーのみをサブスクライブできます。
> - 通知ルールの作成の一環として AWS Chatbot クライアントを作成することはできません。 AWS Chatbot (Slack) または AWS Chatbot (Microsoft Teams) を選択すると、AWS Chatbot でクライアントを設定するように指示するボタンが表示されます。このオプションを選択すると、 AWS Chatbot コンソールが開きます。詳細については、「Slack チャネルの AWS Chatbot クライアントを設定する」を参照してください。

- 既存の Amazon SNS トピックをターゲットとして使用する場合は、そのトピックに存在する可能性のある他のポリシーに加えて、 AWS CodeStar Notifications に必要なポリシーを追加する必要があります。詳細については、「通知用に Amazon SNS トピックを設定する」および「通知の内容とセキュリティについて」を参照してください。

8. [送信] を選択し、通知ルールを確認します。

> **Note**
>
> ユーザーは、通知を受け取る前に、ルールのターゲットとして指定した Amazon SNS トピックにサブスクライブしてサブスクライブを確認する必要があります。詳細については、「通知に使用する Amazon SNS トピックにユーザーをサブスクライブするには」を参照してください。

通知ルールを作成するには (AWS CLI)

1. ターミナルまたはコマンドプロンプトで、create-notification rule コマンドを実行して JSON スケルトンを生成します。

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

ファイルには任意の名前を付けることができます。この例では、ファイルの名前を *rule.json* とします。

2. プレーンテキストエディタで JSON ファイルを開き、これを編集してルールに必要なリソース、イベントタイプ、および Amazon SNS ターゲットを含めます。

次の例は、ID *123456789012* の AWS アカウントの *MyDemoRepo* という名前のリポジトリ**MyNotificationRule**に対して という名前の通知ルールを示しています。ブランチとタグが作成されると、完全な詳細タイプの通知は、*MyNotificationTopic* という Amazon SNS トピックに送信されます。

```
{
    "Name": "MyNotificationRule",
```

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

ファイルを保存します。

3. 先ほど編集したファイルを使用して、ターミナルまたはコマンドラインで create-notification-rule コマンドを再度実行し、通知ルールを作成します。

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

4. 成功すると、次に示すような通知ルールの ARN がコマンドから返されます。

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

通知ルールのイベントタイプを一覧表示するには (AWS CLI)

1. ターミナルまたはコマンドラインプロンプトで、list-event-types コマンドを実行します。--filters オプションを使用して、応答を特定のリソースタイプまたは他の属性に制限できます。例えば、次のコマンドは CodeDeploy アプリケーションのイベントタイプのリストを返します。

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

2. このコマンドでは、次のような出力が生成されます。

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

通知ルールにタグを追加するには (AWS CLI)

1. ターミナルまたはコマンドラインプロンプトで、tag-resource コマンドを実行します。例えば、次のコマンドを使用して、*Team* という名前と *Li_Juan* という値を持つタグキーと値のペアを追加します。

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

2. このコマンドでは、次のような出力が生成されます。

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

通知ルールの表示

デベロッパーツールコンソールまたは を使用して AWS CLI 、 AWS リージョン内のすべてのリソースのすべての通知ルールを表示できます。各通知ルールの詳細を表示することもできます。通知ルールを作成するプロセスとは異なり、リソースのリソースページに移動する必要はありません。

通知ルールを表示するには (コンソール)

1. https://console.aws.amazon.com/codesuite/settings/notifications で AWS デベロッパーツールコンソールを開きます。
2. ナビゲーションバーで、[Settings (設定)] を展開し、[Notifications rules (通知ルール)] を選択します。
3. 通知ルールで、現在サインイン AWS リージョン している AWS アカウント の リソース用に設定されたルールのリストを確認します。セレクタを使用して AWS リージョンを変更します。
4. 通知ルールの詳細を表示するには、リストからルールを選択し、[詳細を表示] を選択します。リストで名前を選択することもできます。

通知ルールのリストを表示するには (AWS CLI)

1. ターミナルまたはコマンドプロンプトで、 list-notification-rules コマンドを実行して、指定された AWS リージョンのすべての通知ルールを表示します。

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

2. 成功すると、このコマンドは、次のような AWS リージョン内の各通知ルールの ID と ARN を返します。

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

```
    ]
}
```

通知ルールの詳細を表示するには (AWS CLI)

1. ターミナルまたはコマンドプロンプトで、describe-notification-rule コマンドを実行します。実行する際に通知ルールの ARN を指定します。

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

2. 成功すると、コマンドは以下のような出力を返します。

```
{
    "LastModifiedTimestamp": 1569199844.857,
    "EventTypes": [
        {
            "ServiceName": "CodeCommit",
            "EventTypeName": "Branches and tags: Created",
            "ResourceType": "Repository",
            "EventTypeId": "codecommit-repository-branches-and-tags-created"
        }
    ],
    "Status": "ENABLED",
    "DetailType": "FULL",
    "Resource": "arn:aws:codecommit:us-east-1:123456789012:MyDemoRepo",
    "Arn": "arn:aws:codestar-notifications:us-east-1:123456789012:notificationrule/
dc82df7a-EXAMPLE",
    "Targets": [
        {
            "TargetStatus": "ACTIVE",
            "TargetAddress": "arn:aws:sns:us-
east-1:123456789012:MyNotificationTopic",
            "TargetType": "SNS"
        }
    ],
    "Name": "MyNotificationRule",
    "CreatedTimestamp": 1569199844.857,
    "CreatedBy": "arn:aws:iam::123456789012:user/Mary_Major"
}
```

通知ルールのタグのリストを表示するには (AWS CLI)

1. ターミナルまたはコマンドプロンプトで、list-tags-for-resource コマンドを実行し、指定した通知ルール ARN のすべてのタグを表示します。

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

2. 正常に完了した場合、このコマンドは以下のような出力を返します。

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

通知ルールの編集

通知ルールを編集して、その名前、通知を送信する対象のイベント、詳細タイプまたは通知の送信先のターゲットを変更できます。デベロッパーツールコンソールまたは を使用して AWS CLI 、通知ルールを編集できます。

通知ルールを編集するには (コンソール)

1. https://console.aws.amazon.com/codesuite/settings/notifications で AWS デベロッパーツールコンソールを開きます。
2. ナビゲーションバーで、[Settings (設定)] を展開し、[Notifications rules (通知ルール)] を選択します。
3. 通知ルールで、現在サインイン AWS リージョン している の AWS アカウント内のリソース用に設定されたルールを確認します。セレクタを使用して AWS リージョンを変更します。
4. リストからルールを選択し、[編集] を選択します。変更を行ってから、[送信] を選択します。

通知ルールを編集するには (AWS CLI)

1. ターミナルまたはコマンドプロンプトで、 describe-notification-rule コマンド を実行し、通知ルールの構造を表示します。
2. update-notification rule コマンドを実行して JSON スケルトンを生成し、それをファイルに保存します。

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

ファイルには任意の名前を付けることができます。この例では、ファイルは *update.json* です。

3. プレーンテキストエディタで JSON ファイルを開き、そのルールを変更します。

次の例は、ID *123456789012* の AWS アカウントの *MyDemoRepo* という名前のリポジトリ**MyNotificationRule**に対して という名前の通知ルールを示しています。ブランチとタグが作成されると、通知は、*MyNotificationTopic* という Amazon SNS トピックに送信されます。ルール名は、*MyNewNotificationRule* に変更されます。

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

ファイルを保存します。

4. 先ほど編集したファイルを使用して、ターミナルまたはコマンドラインで update-notification-rule コマンドを再度実行し、通知ルールを更新します。

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

5. 成功すると、次に示すような通知ルールの Amazon リソースネーム (ARN) がコマンドから返されます。

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

通知ルールからタグを削除するには (AWS CLI)

1. ターミナルまたはコマンドラインプロンプトで、untag-resource コマンドを実行します。例えば、次のコマンドは *Team* という名前のタグを削除します。

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

2. 成功した場合、このコマンドは何も返しません。

関連情報

- 通知ルールのターゲットの追加または削除
- 通知ルールの通知の有効化または無効化
- Events

通知ルールの通知の有効化または無効化

通知ルールを作成すると、通知はデフォルトで有効になります。ルールを削除して通知を送信しないようにする必要はありません。通知ステータスを変更するだけです。

通知ルールの通知ステータスを変更するには (コンソール)

1. https://console.aws.amazon.com/codesuite/settings/notifications で AWS デベロッパーツールコンソールを開きます。
2. ナビゲーションバーで、[Settings (設定)] を展開し、[Notifications rules (通知ルール)] を選択します。
3. 通知ルールで、現在サインイン AWS リージョン している の AWS アカウント内のリソース用に設定されたルールを確認します。セレクタを使用して AWS リージョンを変更します。
4. 有効または無効にする通知ルールを見つけ、そのルールを選択して詳細を表示します。
5. Notification (通知) ステータスで、スライダーを選択してルールのステータスを変更します。

- [通知を送信する]: これがデフォルト値です。
- [Notifications paused (通知が一時停止されました)]: 指定されたターゲットに通知は送信されません。

通知ルールの通知ステータスを変更するには (AWS CLI)

1. 通知ルールを編集するには (AWS CLI) の手順に従って、通知ルールの JSON を取得します。
2. [Status] フィールドを [ENABLED] (デフォルト) または [DISABLED] (通知なし) に編集し、update-notification-rule コマンドを実行してステータスを変更します。

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

通知ルールの削除

リソースに対して設定できる通知ルールは 10 個のみであるため、不要になったルールは削除することを検討してください。デベロッパーツールコンソールまたは を使用して AWS CLI 、通知ルールを削除できます。

> **Note**
>
> 通知ルールの削除を元に戻すことはできませんが、再作成することはできます。通知ルールを削除しても、ターゲットは削除されません。

通知ルールを削除するには (コンソール)

1. https://console.aws.amazon.com/codesuite/settings/notifications で AWS デベロッパーツールコンソールを開きます。
2. ナビゲーションバーで、[Settings (設定)] を展開し、[Notifications rules (通知ルール)] を選択します。
3. 通知ルールで、現在サインイン AWS リージョン している の AWS アカウント内のリソース用に設定されたルールを確認します。セレクタを使用して AWS リージョンを変更します。
4. 通知ルールを選択し、[削除] を選択します。
5. 「**delete**」と入力後、[削除] を選択します。

通知ルールを削除するには (AWS CLI)

1. ターミナルまたはコマンドプロンプトで、delete-notification-rule コマンドを実行します。実行する際に通知ルールの ARN を指定します。

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

2. 成功すると、次に示すように、削除された通知ルールの ARN がコマンドから返されます。

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

通知ルールのターゲットの使用

通知ルールのターゲットとは送信先であり、通知ルールのイベント条件が満たされたときに通知を送信する先を定義します。Slack または Microsoft Teams チャネル用に設定された Amazon SNS トピックと AWS Chatbot クライアントを選択できます。通知ルールの作成の一環として、Amazon SNS トピックをターゲットとして作成できます (推奨)。通知ルールと同じ AWS リージョンにある既存の Amazon SNS トピックを選択することもできますが、必要なポリシーで設定する必要があります。 AWS Chatbot クライアントをターゲットとして使用する場合は、まず AWS Chatbot でそのクライアントを作成する必要があります。

通知の到達範囲を拡張する場合は、通知が Amazon Chime チャットルームに送信されるように、通知と AWS Chatbot の統合を手動で設定できます。その後、その AWS Chatbot クライアント用に設定された Amazon SNS トピックを通知ルールのターゲットとして選択できます。詳細については、「Chatbot および Amazon Chime AWS と通知を統合するには」を参照してください。

デベロッパーツールコンソールまたは を使用して AWS CLI 、通知ターゲットを管理できます。コンソールまたは を使用して AWS CLI 、Amazon SNS トピックと AWS Chatbot クライアントをターゲットとして作成および設定できます。ターゲットとして設定した Amazon SNS トピックと AWS Chatbot の統合を設定することもできます。これにより、Amazon Chime チャットルームに通知を送信できます。詳細については、「通知と AWS Chatbot の統合を設定する」を参照してください。

トピック

- 通知ルールのターゲットの作成または設定

- 通知ルールのターゲットの表示
- 通知ルールのターゲットの追加または削除
- 通知ルールのターゲットの削除

通知ルールのターゲットの作成または設定

通知ルールのターゲットは、Slack または Microsoft Teams チャネル用に設定された Amazon SNS トピックまたは AWS Chatbot クライアントです。

ターゲットとしてクライアントを選択する前に、 AWS Chatbot クライアントを作成する必要があります。 AWS Chatbot クライアントを通知ルールのターゲットとして選択すると、通知を Slack または Microsoft Teams チャネルに送信するために必要なすべてのポリシーを使用して、その AWS Chatbot クライアントに Amazon SNS トピックが設定されます。既存の Amazon SNS トピックを AWS Chatbot クライアント用に設定する必要はありません。

通知ルールを作成するときに、デベロッパーツールコンソールで Amazon SNS 通知ルールターゲットを作成できます。そのトピックへの通知の送信を許可するポリシーが適用されます。これは、通知ルールのターゲットを作成する最も簡単な方法です。詳細については、「通知ルールの作成」を参照してください。

既存の Amazon SNS トピックを使用する場合は、リソースがそのトピックに通知を送信できるようにするアクセスポリシーを使用して設定する必要があります。例については、通知用に Amazon SNS トピックを設定するを参照してください。

> **Note**
>
> 新しいトピックを作成する代わりに既存の Amazon SNS トピックを使用する場合は、[Targets (ターゲット)] でその ARN を選択します。トピックに適切なアクセスポリシーがあり、リソースに関する情報を表示できるユーザーのみがサブスクライバーリストに含まれていることを確認します。Amazon SNS トピックが 2019 年 11 月 5 日より前に CodeCommit 通知に使用されたトピックである場合、CodeStar Notifications に必要な AWS CodeStar CodeCommit への発行を許可するポリシーが含まれます。これらのトピックの使用は非推奨です。そのエクスペリエンス用に作成されたポリシーを使用する場合は、既存のポリシーに加えて、 AWS CodeStar Notifications に必要なポリシーを追加する必要があります。詳細については、「通知用に Amazon SNS トピックを設定する」および「通知の内容とセキュリティについて」を参照してください。

通知の到達範囲を拡張する場合は、通知が Amazon Chime チャットルームに送信されるように、通知と AWS Chatbot の統合を手動で設定できます。詳細については、「ターゲット」および「Chatbot および Amazon Chime AWS と通知を統合するには」を参照してください。

通知ルールのターゲットとして使用する既存の Amazon SNS トピックを設定するには (コンソール)

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/sns/v3/home で Amazon SNS コンソールを開きます。
2. ナビゲーションバーで、[トピック] を選択します。トピックを選択し、[編集] を選択します。
3. [アクセスポリシー]を展開し、アドバンストを選択します。
4. JSON エディタで、ポリシーに次のポリシーステートメントを追加します。トピック ARN、AWS リージョン AWS アカウント ID、トピック名を含めます。

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

このポリシーステートメントは、次のようになります。

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

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

5. [Save changes] (変更の保存) をクリックします。
6. [サブスクリプション] で、トピックサブスクライバーのリストを確認します。この通知ルールのターゲットに合わせて、受信者を追加、編集、または削除します。サブスクライバーのリストには、リソースに関する情報を表示できるユーザーだけが記載されていることを確認します。詳細については、「通知の内容とセキュリティについて」を参照してください。

ターゲットとして使用する Slack で AWS Chatbot クライアントを作成するには

1. 「AWS Chatbot 管理者ガイド」の「AWS Chatbot を Slack で設定する」の手順に従ってください。この場合、通知との統合を最適化するために以下の選択肢を検討してください。

- IAM ロールを作成するときに、このロールの目的を端的に示すロール名 (**AWSCodeStarNotifications-Chatbot-Slack-Role** など) を選択します。これにより、以後、ロールの使用目的がわかりやすくなります。
- SNS トピックでは、トピックまたは AWS リージョンを選択する必要はありません。 AWS Chatbot クライアントをターゲットとして選択すると、通知ルールの作成プロセスの一環として、必要なすべてのアクセス許可を持つ Amazon SNS トピックが AWS Chatbot クライアント用に作成および設定されます。

2. クライアントの作成プロセスを完了します。通知ルールの作成時に、このクライアントをターゲットとして選択できます。詳細については、「通知ルールの作成」を参照してください。

> **Note**
>
> 設定後に AWS Chatbot クライアントから Amazon SNS トピックを削除しないでください。削除すると、Slack に通知が送信されなくなります。

ターゲットとして使用する Microsoft Teams で AWS Chatbot クライアントを作成するには

1. 「AWS Chatbot 管理者ガイド」の「AWS Chatbot を Microsoft Teams で設定する」の手順に従ってください。この場合、通知との統合を最適化するために以下の選択肢を検討してください。

   - IAM ロールを作成するときに、このロールの目的を端的に示すロール名 (**AWSCodeStarNotifications-Chatbot-Microsoft-Teams-Role** など) を選択します。これにより、以後、ロールの使用目的がわかりやすくなります。
   - SNS トピックでは、トピックまたは AWS リージョンを選択する必要はありません。 AWS Chatbot クライアントをターゲットとして選択すると、通知ルールの作成プロセスの一環として、必要なすべてのアクセス許可を持つ Amazon SNS トピックが AWS Chatbot クライアント用に作成および設定されます。

2. クライアントの作成プロセスを完了します。通知ルールの作成時に、このクライアントをターゲットとして選択できます。詳細については、「通知ルールの作成」を参照してください。

> **Note**
>
> 設定後に AWS Chatbot クライアントから Amazon SNS トピックを削除しないでください。削除すると、Microsoft Teams に通知が送信されなくなります。

通知ルールのターゲットの表示

Amazon SNS コンソールではなくデベロッパーツールコンソールを使用して、 AWS リージョン内のすべてのリソースのすべての通知ルールターゲットを表示できます。通知ルールのターゲットの詳細を表示することもできます。

通知ルールのターゲットを表示するには (コンソール)

1. https://console.aws.amazon.com/codesuite/settings/notifications で AWS デベロッパーツールコンソールを開きます。
2. ナビゲーションバーで、[Settings (設定)] を展開し、[Notifications rules (通知ルール)] を選択します。
3. 通知ルールターゲットで、現在サインイン AWS リージョン している の AWS アカウント で通知ルールが使用するターゲットのリストを確認します。セレクタを使用して AWS リージョンを変更します。ターゲットのステータスが [Unreachable (到達不能)] と表示された場合は、調査が必要になる場合があります。詳細については、「トラブルシューティング」を参照してください。

通知ルールのターゲットを一覧表示するには (AWS CLI)

1. ターミナルまたはコマンドプロンプトで、list-targets コマンドを実行して、指定した AWS リージョンのすべての通知ルールのターゲットを一覧表示します。

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

2. 成功すると、このコマンドは、次のような AWS リージョン内の各通知ルールの ID と ARN を返します。

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

```
            "TargetType": "AWSChatbotSlack"
        },
        {
            "TargetAddress": "arn:aws:sns:us-
east-2:123456789012:MySNSTopicForNotificationsAboutMyDemoRepo",
            "TargetType": "SNS",
            "TargetStatus": "ACTIVE"
        }
    ]
}
```

通知ルールのターゲットの追加または削除

通知ルールを編集して、通知を送信する先のターゲットを変更できます。デベロッパーツールコンソール、、または を使用して AWS CLI 、通知ルールのターゲットを変更できます。

通知ルールのターゲットを変更するには (コンソール)

1. https://console.aws.amazon.com/codesuite/settings/notifications で AWS デベロッパーツールコンソールを開きます。
2. ナビゲーションバーで、[Settings (設定)] を展開し、[Notifications rules (通知ルール)] を選択します。
3. 通知ルールで、現在サインイン AWS リージョン している の AWS アカウントでリソース用に設定されたルールのリストを確認します。セレクタを使用して AWS リージョンを変更します。
4. ルールを選択し、[編集] を選択します。
5. [Targets (ターゲット)] で、次のいずれかの操作を行います。
   - 別のターゲットを追加するには、ターゲットの追加を選択し、リストから追加する Amazon SNS トピックまたは AWS Chatbot (Slack) または AWS Chatbot (Microsoft Teams) クライアントを選択します。[Create SNS topic (SNS トピックを作成する)] を選択してトピックを作成し、ターゲットとして追加することもできます。1 つの通知ルールに最大 10 個のターゲットを設定できます。
   - ターゲットを削除するには、削除するターゲットの横にある [Remove target (ターゲットの削除)] を選択します。
6. [Submit] を選択してください。

通知ルールにターゲットを追加するには (AWS CLI)

1. ターミナルまたはコマンドプロンプトで、subscribe コマンドを実行してターゲットを追加します。例えば、次のコマンドは、通知ルールのターゲットとして Amazon SNS トピックを追加します。

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

2. 成功すると、次に示すように、更新された通知ルールの ARN がコマンドから返されます。

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

通知ルールからターゲットを削除するには (AWS CLI)

1. ターミナルまたはコマンドプロンプトで、unsubscribe コマンドを実行してターゲットを削除します。例えば、次のコマンドは、通知ルールのターゲットとしての Amazon SNS トピックを削除します。

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

2. 成功すると、次に示すように、更新された通知ルールの ARN および削除されたターゲットに関する情報がコマンドから返されます。

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

関連情報

- 通知ルールの編集
- 通知ルールの通知の有効化または無効化

通知ルールのターゲットの削除

ターゲットが不要になった場合は、削除できます。リソースには通知ルールのターゲットを 10 個しか設定できないため、不要なターゲットを削除することで、その空いたスペースに他の必要なターゲットを追加できます。

> **Note**
>
> 通知ルールのターゲットを削除すると、それをターゲットとして使用するように設定されているすべての通知ルールからターゲットが削除されます。ただし、ターゲット自体は削除されません。

通知ルールのターゲットを削除するには (コンソール)

1. https://console.aws.amazon.com/codesuite/settings/notifications で AWS デベロッパーツールコンソールを開きます。
2. ナビゲーションバーで、[Settings (設定)] を展開し、[Notifications rules (通知ルール)] を選択します。
3. 通知ルールターゲットで、現在サインイン AWS リージョン している の AWS アカウントでリソース用に設定されたターゲットのリストを確認します。セレクタを使用して AWS リージョンを変更します。
4. 通知ルールのターゲットを選択し、[削除] を選択します。
5. 「**delete**」と入力後、[削除] を選択します。

通知ルールのターゲットを削除するには (AWS CLI)

1. ターミナルまたはコマンドプロンプトで、delete-target コマンドを実行します。実行する際にターゲットの ARN を指定します。例えば、次のコマンドは、Amazon SNS トピックを使用するターゲットを削除します。

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

2. 成功すると、コマンドは何も返しません。失敗すると、コマンドはエラーを返します。最も一般的なエラーは、トピックが 1 つ以上の通知ルールのターゲットになっている場合です。

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

`--force-unsubscribe-all` パラメータを使用すると、そのトピックをターゲットとして使用するように設定されているすべての通知ルールからターゲットを削除できます。さらにターゲット自体も削除できます。

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

通知と AWS Chatbot の統合を設定する

AWS Chatbot は、DevOps およびソフトウェア開発チームが Amazon Chime チャットルーム、Slack チャネル、Microsoft Team チャネルを使用して、 の運用イベントをモニタリングして対応できるようにする AWS サービスです AWS クラウド。イベントに関する通知が、選択した Amazon Chime ルーム、Slack チャネル、または Microsoft Teams チャネルに表示されるように、通知ルールターゲットと AWS Chatbot の統合を設定できます。詳細については、「AWS Chatbot ドキュメント」を参照してください。

AWS Chatbot との統合を設定する前に、通知ルールとルールターゲットを設定する必要があります。詳細については、「セットアップ」および「通知ルールの作成」を参照してください。また、AWS Chatbot で Slack チャンネル、Microsoft Teams チャネル、または Amazon Chime チャットルームも設定する必要があります。詳細については、これらのサービスのドキュメントを参照してください。

トピック

- Slack チャネルの AWS Chatbot クライアントを設定する
- Microsoft Teams チャネルの AWS Chatbot クライアントを設定する
- Slack または Amazon Chime のクライアントの手動設定

Slack チャネルの AWS Chatbot クライアントを設定する

AWS Chatbot クライアントをターゲットとして使用する通知ルールを作成できます。Slack チャネルのクライアントを作成すると、このクライアントを通知ルールの作成ワークフローでターゲットとして直接使用できます。これは、Slack チャネルに表示される通知を設定する最も簡単な方法です。

ターゲットとして使用する Slack で AWS Chatbot クライアントを作成するには

1. 「AWS Chatbot 管理者ガイド」の「AWS Chatbot を Slack で設定する」の手順に従ってください。この場合、通知との統合を最適化するために以下の選択肢を検討してください。

   - IAM ロールを作成するときに、このロールの目的を端的に示すロール名 (**AWSCodeStarNotifications-Chatbot-Slack-Role** など) を選択します。これにより、以後、ロールの使用目的がわかりやすくなります。
   - SNS トピックでは、トピックまたは AWS リージョンを選択する必要はありません。 AWS Chatbot クライアントをターゲットとして選択すると、通知ルールの作成プロセスの一環として、必要なすべてのアクセス許可を持つ Amazon SNS トピックが AWS Chatbot クライアント用に作成および設定されます。
2. クライアントの作成プロセスを完了します。通知ルールの作成時に、このクライアントをターゲットとして選択できます。詳細については、「通知ルールの作成」を参照してください。

> **Note**
>
> 設定後に AWS Chatbot クライアントから Amazon SNS トピックを削除しないでください。削除すると、Slack に通知が送信されなくなります。

Microsoft Teams チャネルの AWS Chatbot クライアントを設定する

AWS Chatbot クライアントをターゲットとして使用する通知ルールを作成できます。Microsoft Teams チャネルのクライアントを作成すると、このクライアントを通知ルールの作成ワークフローでターゲットとして直接使用できます。これは、Microsoft Teams チャネルに表示される通知を設定する最も簡単な方法です。

ターゲットとして使用する Microsoft Teams で AWS Chatbot クライアントを作成するには

1. 「AWS Chatbot 管理者ガイド」の「AWS Chatbot を Microsoft Teams で設定する」の手順に従ってください。この場合、通知との統合を最適化するために以下の選択肢を検討してください。

- IAM ロールを作成するときに、このロールの目的を端的に示すロール名 (**AWSCodeStarNotifications-Chatbot-Microsoft-Teams-Role** など) を選択します。これにより、以後、ロールの使用目的がわかりやすくなります。
- SNS トピックでは、トピックまたは AWS リージョンを選択する必要はありません。 AWS Chatbot クライアントをターゲットとして選択すると、通知ルールの作成プロセスの一環として、必要なすべてのアクセス許可を持つ Amazon SNS トピックが AWS Chatbot クライアント用に作成および設定されます。

2. クライアントの作成プロセスを完了します。通知ルールの作成時に、このクライアントをターゲットとして選択できます。詳細については、「通知ルールの作成」を参照してください。

> **Note**
>
> 設定後に AWS Chatbot クライアントから Amazon SNS トピックを削除しないでください。削除すると、Microsoft Teams に通知が送信されなくなります。

Slack または Amazon Chime のクライアントの手動設定

Slack や Amazon Chime と通知との統合を直接作成することを選択できます。これは、Amazon Chime チャットルームへの通知を設定するための唯一の方法です。この統合を手動で設定する場合は、通知ルールのターゲットとして以前に設定した Amazon SNS トピックを使用する AWS Chatbot クライアントを作成します。

AWS Chatbot および slack と通知を手動で統合するには

1. https://console.aws.amazon.com/codesuite/settings/notifications で AWS デベロッパーツールコンソールを開きます。
2. [Settings (設定)]、[Notification rules (通知ルール)] の順に選択します。
3. [通知ルールのターゲット] で、ターゲットを検索してコピーします。

> **Note**
>
> そのターゲットと同じ Amazon SNS トピックを使用する通知ルールを複数設定できます。これはメッセージングを統合するのに役立ちますが、サブスクリプションリストが 1 つの通知ルールまたはリソースを対象としている場合、意図しない結果が生じることがあります。

4. https://console.aws.amazon.com/chatbot/ で AWS Chatbot コンソールを開きます。
5. [Configure new client]、[Slack] の順に選択します。
6. [設定] を選択します。
7. Slack ワークスペースにサインインします。
8. 選択内容を確認するメッセージが表示されたら、[Allow (許可)] を選択します。
9. [Configure new channel] を選択します。
10. [Configuration details] で、[Configuration name] にクライアント名を入力します。これは、通知ルールの作成時に AWS Chatbot (Slack) ターゲットタイプの使用可能なターゲットのリストに表示される名前です。
11. [Configure Slack Channel] (Slack チャネルの設定) の [Channel type] (チャネルタイプ) で、統合するチャネルのタイプに応じて [Public] (パブリック) または [Private] (プライベート) を選択します。
    - [Public channel (パブリックチャネル)] で、Slack チャネルの名前をリストから選択します。
    - [Private channel ID (プライベートチャネル ID)] に、チャネルコードまたは URL を入力します。
12. [IAM permissions] (IAM アクセス許可) の [Role] (ロール) で、[Create an IAM role using a template] (テンプレートを使用して IAM ロールを作成する) を選択します。[ポリシーテンプレート] で、[通知のアクセス許可] を選択します。[ロール名] に、このロールの名前（**`AWSCodeStarNotifications-Chatbot-Slack-Role`** など）を入力します。[ポリシーテンプレート] で、[通知のアクセス許可] を選択します。
13. SNS トピックの SNS リージョンで、通知ルールターゲットを作成した AWS リージョン を選択します。[SNS topics] で、通知ルールのターゲットとして設定した Amazon SNS トピックの名前を選択します。

    > **Note**
    >
    > このステップは、このクライアントをターゲットとして使用する通知ルールを作成する場合は必要ありません。

14. [設定] を選択します。

> **Note**
>
> プライベートチャンネルとの統合を設定した場合、そのチャンネルに通知が表示されるには AWS Chatbot をチャンネルに招待する必要があります。詳細については、「AWS Chatbot ドキュメント」を参照してください。

15. (オプション) 統合をテストするには、ターゲットとして Amazon SNS トピックを使用するように設定された通知ルールのイベントタイプに対応するリソースを変更します。例えば、プルリクエストに対してコメントが作成されたときに通知を送信するように設定された通知ルールがある場合は、プルリクエストにコメントし、ブラウザで Slack チャネルを監視して、通知がいつ表示されるかを確認します。

Chatbot および Amazon Chime AWS と通知を統合するには

1. https://console.aws.amazon.com/codesuite/settings/notifications で AWS デベロッパーツールコンソールを開きます。
2. [Settings (設定)]、[Notification rules (通知ルール)] の順に選択します。
3. [通知ルールのターゲット] で、ターゲットを検索してコピーします。

> **Note**
>
> そのターゲットと同じ Amazon SNS トピックを使用する通知ルールを複数設定できます。これはメッセージングを統合するのに役立ちますが、サブスクリプションリストが 1 つの通知ルールまたはリソース用である場合、意図しない結果が生じることがあります。

4. Amazon Chime で、統合用に設定するチャットルームを開きます。
5. 右上の歯車アイコンを選択して、[Manage webhooks] を選択します。
6. [Manage webhooks (ウェブフックの管理)] ダイアログボックスで [新規] を選択し、ウェブフックの名前を入力して [作成] を選択します。
7. Webhook が表示されることを確認し、[Copy webhook URL (Webhook URL のコピー)] を選択します。
8. https://console.aws.amazon.com/chatbot/ で AWS Chatbot コンソールを開きます。
9. [Configure new client] (新しいクライアントを設定) 、[Amazon Chime] の順に選択します。
10. [Configuration details] で、[Configuration name] にクライアント名を入力します。

11. [Webhook URL] で、URL を貼り付けます。[Webhook description (Webhook の説明)] に、オプションの説明を入力します。
12. [IAM permissions] (IAM アクセス許可) の [Role] (ロール) で、[Create an IAM role using a template] (テンプレートを使用して IAM ロールを作成する) を選択します。[ポリシーテンプレート] で、[通知のアクセス許可] を選択します。[ロール名] に、このロールの名前（**AWSCodeStarNotifications-Chatbot-Chime-Role** など）を入力します。
13. SNS トピックの SNS リージョンで、通知ルールターゲットを作成した AWS リージョン を選択します。[SNS topics (SNS トピック)] で、通知ルールのターゲットとして設定した Amazon SNS トピックの名前を選択します。
14. [設定] を選択します。
15. (オプション) 統合をテストするには、ターゲットとして Amazon SNS トピックを使用するように設定された通知ルールのイベントタイプに対応するリソースを変更します。例えば、プルリクエストに対してコメントが作成されたときに通知を送信するように設定された通知ルールがある場合は、プルリクエストにコメントし、Amazon Chime チャットルームを監視して通知がいつ表示されるかを確認します。

を使用した Logging AWS CodeStar Notifications API コール AWS CloudTrail

AWS CodeStar Notifications 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。CloudTrail は、 のすべての API コールをイベント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、デベロッパーツールコンソールからの呼び出しと、 AWS CodeStar Notifications API オペレーションへのコードの呼び出しが含まれます。証跡を作成する場合は、通知のイベントなど、Amazon 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 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、 AWS CodeStar Notifications に対して行われたリクエスト、リクエスト元の IP アドレス、リクエスト者、リクエスト日時などの詳細を確認できます。

詳細については、AWS CloudTrail ユーザーガイドをご参照ください。

CloudTrail のAWS CodeStar Notifications 情報

CloudTrail は、アカウントの作成 AWS アカウント 時に で有効になります。 AWS CodeStar Notifications でアクティビティが発生すると、そのアクティビティはイベント履歴の他の AWS サービスイベントとともに CloudTrail イベントに記録されます。で最近のイベントを表示、検索、ダ

ウンロードできます AWS アカウント。詳細については、「Viewing events with CloudTrail event history」(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。

AWS CodeStar Notifications 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、証跡を作成します。追跡により、CloudTrail はログファイルを Amazon S3 バケットに配信できます。デフォルトでは、コンソールで証跡を作成するときに、証跡がすべての 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 Amazon S3 バケットにログファイルを配信します。さらに、CloudTrail ログで収集されたイベントデータをさらに分析して処理するように、他の AWS サービスを設定できます。詳細については、次を参照してください:

- 追跡を作成するための概要
- 「CloudTrail がサポートされているサービスと統合」
- 「CloudTrail の Amazon SNS 通知の設定」
- 「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」

All AWS CodeStar Notifications アクションは CloudTrail によってログに記録され、*AWS CodeStar Notifications API ######*に記載されています。例えば、`CreateNotificationRule`、`Subscribe`、`ListEventTypes` 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、誰がリクエストを生成したかという情報が含まれます。アイデンティティ情報は、以下を判別するのに役立ちます。

- リクエストが root または AWS Identity and Access Management (IAM) ユーザー認証情報を使用して行われたかどうか。
- 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テンポラリ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。

ログファイルエントリの理解

追跡は、指定したAmazon S3バケットにイベントをログファイルとして配信するように設定できます。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、CreateNotificationRule アクションと Subscribe アクションの両方を含む通知ルールの作成を示す CloudTrail ログエントリを示しています。

> **Note**
>
> 通知ログファイルエントリの一部のイベントは、サービスにリンクされたロール AWSServiceRoleForCodeStarNotifications から送信される場合があります。

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

```
    "eventType": "AwsApiCall",
    "apiVersion": "2015-10-07",
    "recipientAccountId": "123456789012"
}
```

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

トラブルシューティング

以下の情報は、通知で発生する一般的な問題のトラブルシューティングに役立つ場合があります。

トピック

リソースに対する通知ルールを作成しようとすると、アクセス許可エラーが表示されます

アクセス許可が十分であることを確認してください。詳細については、「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。

通知ルールを表示できません

問題: デベロッパーツールコンソールで、[設定] から [通知] を選択すると、アクセス許可エラーが表示されます。

解決方法: 通知を表示するために必要なアクセス許可がない可能性があります。CodeCommit や CodePipeline などの AWS デベロッパーツールサービスのほとんどのマネージドポリシーには通知のアクセス許可が含まれていますが、現在通知をサポートしていないサービスには、通知を表示するアクセス許可は含まれません。または、通知の表示を許可しないカスタムポリシーを IAM ユーザーまたはロールに適用することもできます。詳細については、「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。

通知ルールを作成できません

通知ルールの作成に必要なアクセス許可を持っていない可能性があります。詳細については、「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。

アクセスできないリソースに関する通知が届きます

通知ルールを作成してターゲットを追加したときに、受取人がリソースにアクセスできるかどうかは通知機能によって検証されません。アクセスできないリソースに関する通知が届く場合があります。ターゲットのサブスクリプションリストから自分自身を削除できない場合は、削除を依頼してください。

Amazon SNS の通知が届きません

Amazon SNS トピックの問題のトラブルシューティングを行うには、以下を確認します。

- Amazon SNS トピックが通知ルールと同じ AWS リージョンに作成されていることを確認します。
- E メールエイリアスが正しいトピックにサブスクライブされていること、およびサブスクリプションを確認済みであることを確認します。詳細については、「Amazon SNS トピックにエンドポイントをサブスクライブする」を参照してください。
- 該当するトピックに通知をプッシュすることを AWS CodeStar Notifications に許可するようにトピックポリシーが編集されていることを確認します。トピックポリシーには、次のようなステートメントを含める必要があります。

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

詳細については、「通知用に Amazon SNS トピックを設定する」を参照してください。

イベントに関する重複した通知が届きます

複数の通知を受信する最も一般的な理由は以下のとおりです。

- 同じイベントタイプを含む複数の通知ルールをリソースに設定し、これらのルールのターゲットとして複数の Amazon SNS トピックにサブスクライブしている。この問題を解決するには、いずれかのトピックからサブスクリプションを解除するか、通知ルールを編集して重複を削除します。
- 1 つ以上の通知ルールターゲットが AWS Chatbot と統合されており、E メールの受信トレイと Slack チャネル、Microsoft Teams チャネル、または Amazon Chime チャットルームに通知を受信しています。この問題を解決するには、ルールのターゲットである Amazon SNS トピックから E メールアドレスのサブスクリプションを解除し、Slack チャンネル、Microsoft Teams チャネル、または Amazon Chime チャットルームを使用して通知を確認することを検討します。

通知ターゲットのステータスが到達不能と表示される理由を教えてください

ターゲットのステータスには、[Active (アクティブ)] と [Unreachable (到達不能)] の 2 つがあります。[到達不能] は、ターゲットに送信された通知が未到着であることを示します。通知はそのターゲットに引き続き送信され、到着すると、ステータスが [Active (アクティブ)] にリセットされます。

通知ルールのターゲットは、次のいずれかの理由で使用不能になる場合があります。

- リソース (Amazon SNS トピックまたは AWS Chatbot クライアント) が削除されました。通知ルールの別のターゲットを選択した。
- Amazon SNS トピックが暗号化されており、暗号化されたトピックに必要なポリシーがないか、AWS KMS キーが削除されています。詳細については、「通知用に Amazon SNS トピックを設定する」を参照してください。
- 通知に必要なポリシーが Amazon SNS トピックに存在しない。トピックにポリシーがない場合、通知を Amazon SNS トピックに送信することはできません。詳細については、「通知用に Amazon SNS トピックを設定する」を参照してください。
- ターゲットのサポートサービス (Amazon SNS または AWS Chatbot) で問題が発生している可能性があります。

通知とリソースのクォータを引き上げることはできますか

現在、クォータを変更することはできません。「通知のクォータ」を参照してください。

通知のクォータ

次の表に、デベロッパーツールコンソールでの通知のクォータ（制限）を一覧表示します。変更できる制限の詳細については、「AWS のサービスクォータ」を参照してください。

リソース	デフォルトの制限
AWS アカウント内の通知ルールの最大数	1,000
通知ルールのターゲットの最大数	10
リソースの通知ルールの最大数	10

接続とは?

デベロッパーツールコンソールの接続機能を使用して、 などのリソース AWS CodePipeline を外部コードリポジトリに接続 AWS できます。この機能には、独自の API である AWS CodeConnections API リファレンスがあります。各接続は、Bitbucket などのサードパーティーリポジトリに接続するために AWS サービスに付与できるリソースです。例えば、CodePipeline で接続を追加して、サードパーティーのコードリポジトリでコードが変更されたときにパイプラインをトリガーできるようになります。各接続には名前が付けられ、接続を参照するために使用される一意の Amazon Resource Name (ARN) に関連付けられます。

> **Important**
>
> サービス名 AWS CodeStar Connections の名前が変更されました。以前の名前空間 codestar-connections で作成されたリソースは引き続きサポートされます。

接続では何ができますか?

接続を使用して、サードパーティープロバイダーのリソースを次のデベロッパーツールの AWS リソースと統合できます。

- Bitbucket などのサードパーティープロバイダーに接続し、CodePipeline などの AWS リソースとのソース統合としてサードパーティー接続を使用します。
- CodeBuild ビルドプロジェクト、CodeDeploy アプリケーション、およびサードパーティープロバイダーの CodePipeline のパイプラインで、リソース間の接続へのアクセスを均一に管理します。

- CodeBuild ビルドプロジェクト、CodeDeploy アプリケーション、および CodePipeline のパイプライン用のスタックテンプレートで接続 ARN を使用します。保存されたシークレットやパラメーターを参照する必要はありません。

どのサードパーティープロバイダーの接続を作成できますか?

接続では、 AWS リソースを次のサードパーティーリポジトリに関連付けることができます。

- Azure DevOps
- Bitbucket Cloud
- GitHub.com
- GitHub Enterprise Cloud

> **Note**
>
> 現在、GitHub Enterprise Cloud のカスタムドメインはサポートされていません。

- GitHub Enterprise Server
- GitLab.com

> **Important**
>
> GitLab の接続サポートには、バージョン 15.x 以降が含まれています。

- GitLab セルフマネージドのインストール (Enterprise Edition または Community Edition)

接続ワークフローの概要については、「接続を作成または更新するワークフロー」を参照してください。

GitHub などのクラウドプロバイダータイプの接続を作成する手順は、インストール済プロバイダータイプ (GitHub Enterprise Server など) の手順とは異なります。プロバイダーのタイプ別に接続を作成するハイレベルの手順については、「接続の使用」を参照してください。

> **Note**
>
> 欧州 (ミラノ) で接続を使用するには AWS リージョン、以下を行う必要があります。
>
> 1. リージョン固有のアプリをインストールする

2. リージョンを有効にする

このリージョン固有のアプリで、欧州 (ミラノ) リージョンの接続をサポートします。サードパーティープロバイダーのサイトで公開されているアプリであり、他のリージョンの接続をサポートする既存のアプリとは別のものです。このアプリをインストールすることで、このリージョンでのみサービスとデータを共有することをサードパーティープロバイダーに許可します。アプリをアンインストールすることでいつでもアクセス許可を取り消すことができます。
リージョンを有効にしない限り、サービスはデータを処理または保存しません。このリージョンを有効にすることで、データを処理および保存するアクセス許可をサービスに付与したことになります。
リージョンが有効になっていなくても、リージョン固有のアプリがインストールされたままであれば、サードパーティープロバイダーはお客様のデータをサービスと共有できます。したがって、リージョンを無効にしたら、必ずアプリをアンインストールしてください。詳細については、「リージョンの有効化」を参照してください。

接続と AWS のサービス 統合するもの

接続を使用して、サードパーティーのリポジトリを他の AWS のサービスと統合できます。接続のサービス統合を確認するには、「AWS CodeConnections との製品とサービスの統合」を参照してください。

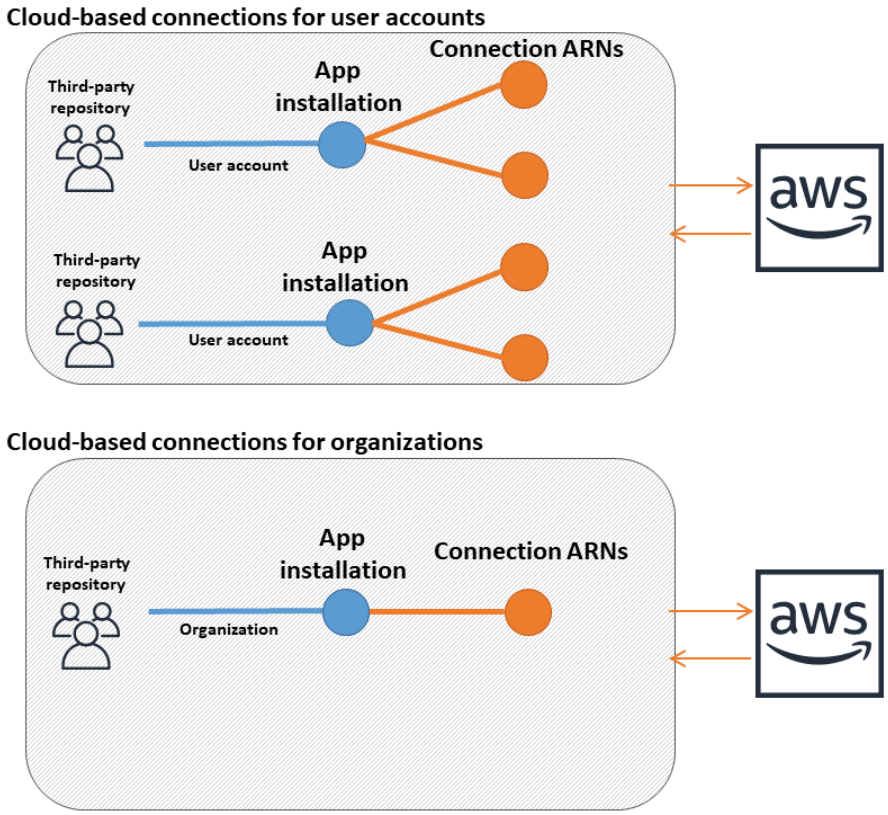
接続はどのように機能しますか？

接続を作成する前に、サードパーティーアカウントで AWS 認証アプリケーションをインストールするか、そのアプリケーションへのアクセス権を提供する必要があります。接続をインストールした後、このインストールを使用するように更新できます。接続を作成すると、サードパーティーアカウントの AWS リソースへのアクセスを許可します。これにより、 接続は、 AWS リソースに代わって、サードパーティーアカウントのソースリポジトリなどのコンテンツにアクセスできます。その後、その接続を他の と共有 AWS のサービス して、リソース間で安全な OAuth 接続を提供できます。

クラウドベースの接続は次のように設定されていますが、ユーザーアカウントまたは組織間では違いがあります。

- ユーザーアカウント: 各クラウドベースのサードパーティーユーザーアカウントには、コネクタアプリがインストールされています。複数の接続をアプリケーションのインストールに関連付けることができます。
- Organizations: 各クラウドベースのサードパーティー組織には、コネクタアプリがインストールされています。組織内の接続の場合、組織内の各組織アカウントへの接続マッピングは 1:1 です。複数の接続をアプリケーションのインストールに関連付けることはできません。組織が接続を操作する方法の詳細については、「」を参照してくださいAWS CodeConnections の接続が組織と連携する方法。

次の図は、クラウドベースの接続がユーザーアカウントまたは組織とどのように連携するかを示しています。



接続は、それらを作成する AWS アカウント によって所有されます。接続は、接続 ID を含む ARN によって識別されます。接続 ID は、変更または再マッピングできない UUID です。接続を削除して再確立すると、新しい接続 ID が作成されるため、新しい接続 ARN が作成されます。つまり、接続 ARN が再利用されることはありません。

新しく作成された接続が `Pending` 状態です。接続のセットアップを完了し、接続を `Pending` 状態から `Available` 状態に移行するには、サードパーティーのハンドシェイク (OAuthフロー) プロセ

スが必要です。これが完了すると、接続は `Available`になり、CodePipeline などの AWS サービスで使用できます。

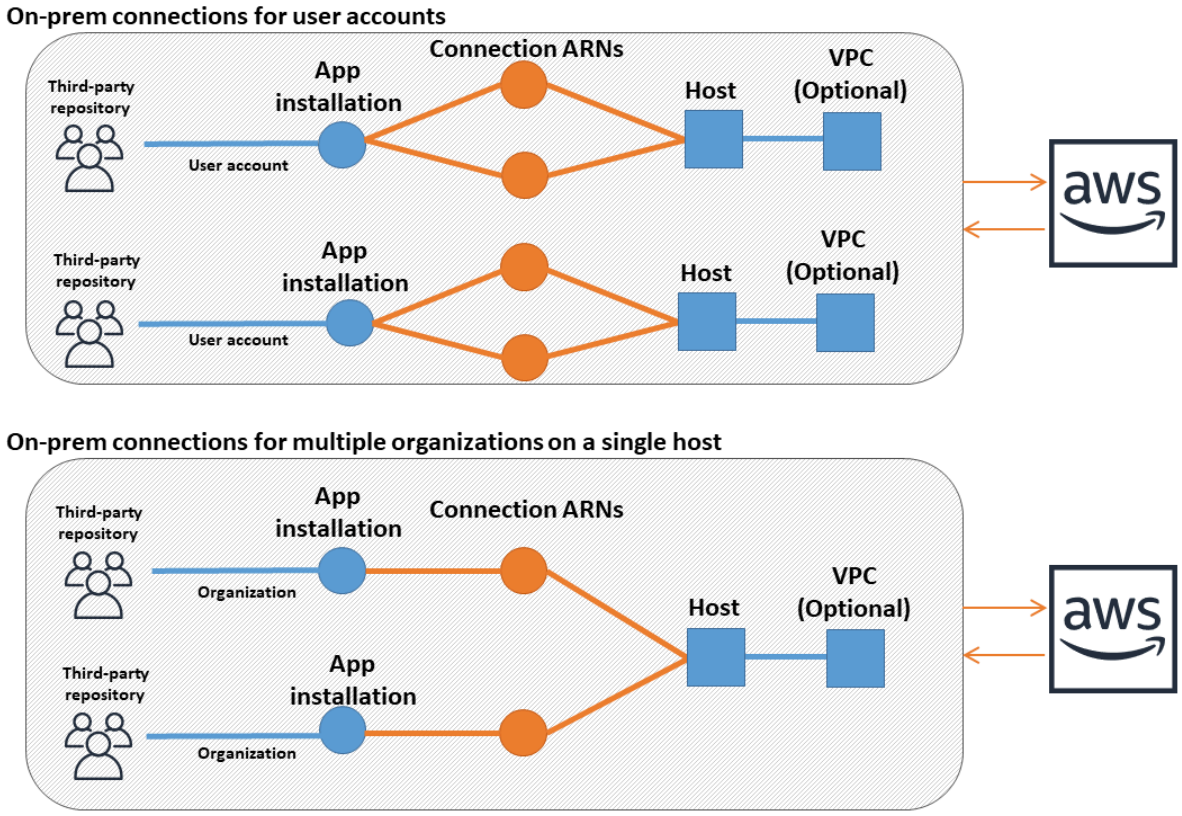
GitHub Enterprise Server や GitLab セルフマネージドなどのインストール済みプロバイダータイプ (オンプレミス) への接続を作成する場合は、接続にホストリソースを使用します。

オンプレミス接続は次のように設定されていますが、ユーザーアカウントまたは組織間では異なります。

- ユーザーアカウント: 各オンプレミスのサードパーティーユーザーアカウントには、コネクタアプリがインストールされています。オンプレミスプロバイダーの複数の接続を 1 つのホストに関連付けることができます。
- Organizations: 各オンプレミスのサードパーティー組織には、コネクタアプリがインストールされています。GitHub Organizations for GitHub Enterprise Server などの組織内のオンプレミス接続の場合、組織内の接続ごとに新しいホストを作成し、ホストのネットワークフィールド (VPC、サブネット IDs、セキュリティグループ IDs) に同じ情報を入力します。組織が接続を操作する方法の詳細については、「」を参照してくださいAWS CodeConnections の接続が組織と連携する方法。
- すべて: オンプレミス接続ごとに、各 VPC は一度に 1 つのホストにのみ関連付けることができます。

いずれの場合も、オンプレミスサーバーの URL を指定する必要があります。さらに、サーバーがプライベート VPC 内にある (インターネット経由でアクセスできない) 場合は、オプションの TLS 証明書情報とともに VPC 情報を提供する必要があります。これらの設定により、CodeConnections はインスタンスと通信でき、このホスト用に作成されたすべての接続で共有されます。たとえば、単一の GitHub Enterprise Server インスタンスの場合、ホストで表される単一のアプリケーションを作成します。次に、ユーザーアカウント設定では、次の図に示すように、アプリのインストールに対応する、そのホストの複数の接続を作成できます。それ以外の場合は、組織に対して、そのホストの単一のアプリケーションインストールと接続を作成します。

次の図は、オンプレミス接続がユーザーアカウントまたは組織とどのように連携するかを示しています。



新しく作成されたホストは Pending 状態です。ホストのセットアップを完了し、ホストを Pending 状態から Available 状態に移行するには、サードパーティーの登録プロセスが必要です。これが完了すると、ホストは Available で、インストール済プロバイダータイプへの接続に使用できます。

接続ワークフローの概要については、「接続を作成または更新するワークフロー」を参照してください。インストール済みプロバイダー用のホスト作成ワークフローの概要については、「ホストを作成または更新するワークフロー」を参照してください。プロバイダーのタイプ別に接続を作成するハイレベルの手順については、「接続の使用」を参照してください。

AWS CodeConnections の接続が組織と連携する方法

GitHub Organizations などのプロバイダーを持つ組織の場合、GitHub アプリを複数の GitHub Organizations にインストールすることはできません。接続には、Github コネクタアプリを使用して組織との 1:1 マッピングがあります。コネクタアプリは、GitHub または GitHub Enterprise Server の組織ごとに分離され、接続が関連付けられている必要があります。

たとえば、同じ GitHub サーバー上の複数の組織と連携するには、組織ごとに個別の接続を作成し、それらの組織に個別の GitHub アプリケーションをインストールする必要があります。ただし、Github 側のターゲットアカウントは同じにすることができます。

接続を作成または更新するワークフロー

接続を作成するときは、サードパーティープロバイダーとの認証ハンドシェイク用に既存のコネクタアプリのインストールを作成または使用します。

接続には、以下のステータスがあります。

- `Pending` -A `pending` 接続は、使用する前に完了 (`available` に移動) する必要があります。
- `Available` - アカウント内の他のリソースやユーザーに `available` 接続を使用または渡すことができます。
- `Error` - `error` 状態の接続は自動的に再試行されます。`available` になるまで使用できません。

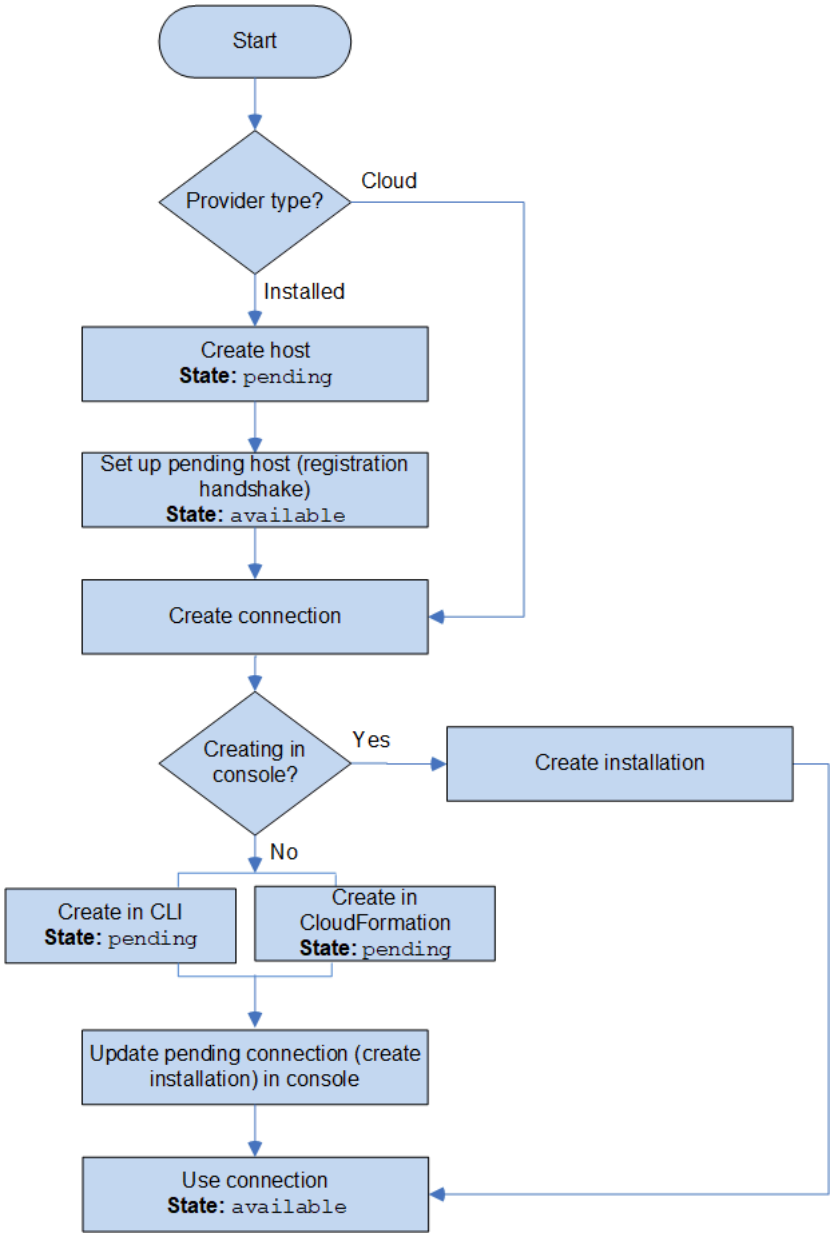
ワークフロー: CLI、SDK、 AWS CloudFormationを使用した接続の作成または更新

CreateConnection API を使用して、 AWS Command Line Interface (AWS CLI)、SDK、または を使用して接続を作成します CloudFormation。作成後、接続は `pending` の状態になります。コンソールの [保留中の接続のセットアップ] オプションを使用して、プロセスを完了します。インストールを作成するか、接続に既存のインストールを使用するかを確認するメッセージがコンソールに表示されます。次に、コンソールでハンドシェイクを完了し、[接続の完了] を選択して、接続を `available` の状態に移行します。

ワークフロー: コンソールとの接続の作成または更新

GitHub Enterprise Server など、インストール済プロバイダータイプへの接続を作成する場合は、最初にホストを作成します。Bitbucket などのクラウドプロバイダーのタイプに接続する場合は、ホストの作成をスキップして、接続の作成を続行します。

コンソールで接続を作成または更新するには、コンソールの [CodePipeline 編集アクション] ページを使用して、サードパーティープロバイダを選択します。 コンソールでは、インストールを作成するか、既存のインストールを使用して接続を作成するように求められます。次に、接続の作成を求められます。コンソールがハンドシェイクを完了し、自動的に `pending` の状態から`available` の状態に移行します。



ホストを作成または更新するワークフロー

インストールされたプロバイダー (オンプレミス) の接続を作成するときは、ホストリソースを使用します。

> **Note**
>
> GitHub Enterprise Server または GitLab セルフマネージドの組織では、使用可能なホストを渡しません。組織内の接続ごとに新しいホストを作成し、ホストのネットワークフィールド (VPC ID、サブネット IDs、セキュリティグループ IDs) に必ず同じ情報を入力する必要があ

ります。詳細については、「組織をサポートするインストール済みプロバイダーの接続とホストのセットアップ」を参照してください。

ホストの各状態は以下のとおりです。

- Pending – pending ホストは作成済みのホストで、使用する前に設定 (available に移行) する必要があります。
- Available - available ホストを使用することも、接続に渡すこともできます。

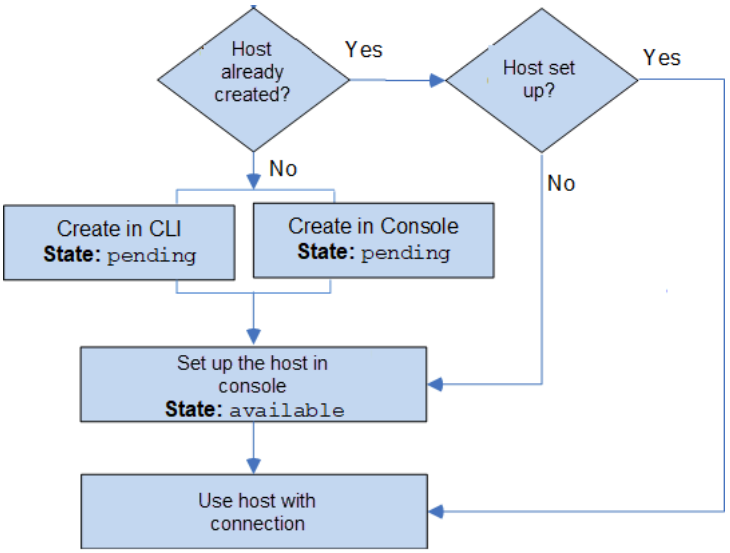
ワークフロー: CLI、SDK、または AWS CloudFormationを使用したホストの作成または更新

CreateHost API を使用して、 AWS Command Line Interface (AWS CLI)、 SDK、または を使用してホストを作成します CloudFormation。作成後、ホストは pending の状態になります。コンソールの [セットアップ] オプションを使用して、プロセスを完了します。

ワークフロー: コンソールを使用したホストの作成または更新

GitHub Enterprise Server や GitLab セルフマネージドなどのインストール済みプロバイダータイプへの接続を作成する場合は、ホストを作成するか、既存のホストを使用します。Bitbucket などのクラウドプロバイダーのタイプに接続する場合は、ホストの作成をスキップして、接続の作成を続行します。

コンソールを使用してホストを設定し、ステータスを pending から available に変更します。



グローバルリソース in AWS CodeConnections

接続はグローバルリソースです。つまり、リソースがすべての AWS リージョンにレプリケートされます。

接続 ARN 形式には作成されたリージョン名が反映されますが、リソースはリージョンに制約されません。接続リソースが作成されたリージョンは、接続リソースデータの更新が制御されるリージョンです。接続リソースデータの更新を制御する API 操作の例として、接続の作成、インストールの更新、接続の削除、接続のタグ付けなどがあります。

接続のホストリソースは、グローバルに利用可能なリソースではありません。ホストリソースは、リソースを作成したリージョンでのみ使用します。

- 接続は 1 回作成するだけで済みます。その後、任意の AWS リージョンで使用できます。
- 接続が作成されたリージョンに問題がある場合、接続リソースデータを制御する API は影響を受けますが、他のすべてのリージョンで接続を正常に使用できます。
- コンソールまたは CLI で接続リソースをリストすると、すべてのリージョンでアカウントに関連付けられているすべての接続リソースが一覧表示されます。
- コンソールまたは CLI でホストリソースをリストすると、リストには、選択したリージョンのアカウントに関連付けられたホストリソースだけが表示されます。
- 関連するホストリソースとの接続がリストされている場合、または CLI で一覧表示されている場合、設定されている CLI リージョンに関係なく、出力はホスト ARN を返します。

接続を開始するにはどうしたらいいですか?

使用を開始するには、次のいくつかのトピックが役立ちます。

- 接続の概念について学びます。
- 必要なリソースをセットアップして、接続の操作を開始します。
- 最初の接続を開始し、それらをリソースに接続します。

接続概念

概念と用語を理解すれば、接続機能の設定と使用が容易になります。デベロッパーツールコンソールの接続機能を使用する際に知っておかなければならないいくつかの概念を次に示します。

インストール

サードパーティーアカウントの AWS アプリケーションのインスタンス。Connector アプリをインストールすると AWS CodeStar AWS 、 はサードパーティーアカウント内のリソースにアクセスできます。インストールは、サードパーティープロバイダーのウェブサイト以外では編集できません。

connection

サードパーティーのソースリポジトリを他の AWS サービスに接続するために使用する AWS リソース。

サードパーティーのリポジトリ

AWS以外のサービスまたは会社が提供するリポジトリ。例えば、Bitbucket リポジトリはサードパーティーのリポジトリです。

プロバイダーのタイプ

接続先のサードパーティソースリポジトリを提供するサービスまたは会社。 AWS リソースを外部プロバイダータイプに接続します。そのソースリポジトリがネットワークおよびインフラストラクチャにインストールされているプロバイダータイプが、インストール済プロバイダータイプです。例えば、GitHub Enterprise Server は、インストール済プロバイダータイプの 1 つです。

ホスト

サードパーティープロバイダーがインストールされているインフラストラクチャを表すリソース。接続は、ホストを使用して、GitHub Enterprise Server などのサードパーティープロバイダがインストールされているサーバーを表します。そのプロバイダータイプへのすべての接続に対して 1 つのホストを作成します。

> **Note**
>
> コンソールを使用して GitHub Enterprise Server への接続を作成すると、コンソールがホストリソースを作成します。これは、コンソールの処理の一部です。

AWS CodeConnections でサポートされているプロバイダーとバージョン

この章では、 AWS CodeConnections がサポートするプロバイダーとバージョンについて説明します。

トピック

Azure DevOps でサポートされているプロバイダータイプ

Azure DevOps で接続アプリを使用できます。

Azure Cloud Hosting などのインストール (ホスト) されたプロバイダータイプはサポートされていません。

Bitbucket でサポートされるプロバイダタイプ

Atlassian Bitbucket Cloud で接続アプリを使用できます。

Bitbucket サーバーなど、インストールされている Bitbucket プロバイダーのタイプはサポートされていません。

GitHub および GitHub Enterprise Cloud でサポートされるプロバイダータイプ

GitHub および GitHub Enterprise Cloud で接続アプリを使用できます。

GitHub Enterprise Server でサポートされているプロバイダーのタイプとバージョン

接続アプリは、サポートされているバージョンの GitHub Enterprise Server で使用できます。サポートされているバージョンのリストについては、「https://enterprise.github.com/releases/」を参照してください。

> **Important**
>
> AWS CodeConnections は、非推奨の GitHub Enterprise Server バージョンをサポートしていません。例えば、 AWS CodeConnections は、リリースの既知の問題のため、GitHub Enterprise Server バージョン 2.22.0 をサポートしていません。接続するには、バージョン 2.22.1 または入手可能な最新のバージョンにアップグレードします。

GitLab.com でサポートされているプロバイダータイプ

GitLab.com. 詳細については、「GitLab への接続を作成する」を参照してください。

> **Important**
>
> GitLab の接続サポートには、バージョン 15.x 以降が含まれています。

GitLab セルフマネージドでサポートされているプロバイダーのタイプ

GitLab セルフマネージドのインストール (Enterprise Edition または Community Edition) で接続を使用できます。詳細については、「GitLab セルフマネージドへの接続を作成する」を参照してください。

AWS CodeConnections との製品とサービスの統合

AWS CodeConnections は、多数の AWS サービスとパートナー製品やサービスと統合されています。以下のセクションの情報は、使用している製品やサービスと統合するための接続の設定に役立ちます。

このサービスを利用する際に役立つ関連リソースは次のとおりです。

トピック

- Amazon CodeGuru Reviewer
- Amazon Q Developer
- Amazon SageMaker
- AWS App Runner
- AWS CloudFormation
- AWS CodeBuild
- AWS CodePipeline
- Service Catalog
- AWS Proton

Amazon CodeGuru Reviewer

CodeGuru Reviewer は、リポジトリコードをモニタリングするためのサービスです。接続を使用して、レビューするコードがあるサードパーティーのリポジトリを関連付けることができます。CodeGuru Reviewer を設定して GitHub リポジトリ内のソースコードをモニタリングし、コードを改善するレコメンデーションを作成できるようにする方法のチュートリアルについては、Amazon CodeGuru Reviewer ユーザーガイドの「Tutorial: monitor source code in a GitHub repository」を参照してください。

Amazon Q Developer

Amazon Q Developer は、生成 AI を活用した会話アシスタントであり、 AWS アプリケーションの理解、構築、拡張、運用に役立ちます。詳細については、「Amazon Q Developer ユーザーガイド」の「What is Amazon Q Developer?」を参照してください。

Amazon SageMaker

Amazon SageMaker は、機械学習言語モデルを構築、トレーニング、デプロイするためのサービスです。GitHub リポジトリへの接続を設定するチュートリアルについては、「Amazon SageMaker 開発者ガイド」の「サードパーティの Git リポジトリを使用する SageMaker MLOps プロジェクトのチュートリアル」を参照してください。

AWS App Runner

AWS App Runner は、 AWS クラウドで、ソースコードまたはコンテナイメージから、スケーラブルでセキュアなウェブアプリケーションに迅速でシンプルな、費用対効果の高い方法で直接デプロイできるサービスです。App Runner の自動統合および配信パイプラインを使用して、リポジトリからアプリケーションコードをデプロイできます。接続を使用して、プライベート GitHub リポジトリから App Runner サービスにソースコードをデプロイできます。詳細については、AWS App Runner デベロッパーガイドの「ソースコードのリポジトリプロバイダー」を参照してください。

AWS CloudFormation

AWS CloudFormation は、 AWS リソースをモデル化してセットアップするのに役立つサービスです。これにより、これらのリソースの管理に費やす時間が減り、 で実行されるアプリケーションに集中する時間が増えます AWS。必要なすべての AWS リソース (Amazon EC2 インスタンスや Amazon RDS DB インスタンスなど) を記述するテンプレートを作成すると、CloudFormation がそれらのリソースのプロビジョニングと設定を処理します。

CloudFormation で Git 同期との接続を使用して、Git リポジトリをモニタリングする同期設定を作成します。スタックデプロイに Git 同期を使用するチュートリアルについては、「 CloudFormation ユーザーガイド」のCloudFormation Git 同期の使用」を参照してください。

CloudFormation の詳細については、CloudFormation コマンドラインインターフェイスユーザーガイド」の「CloudFormation 拡張機能を発行するためのアカウントの登録」を参照してください。 CloudFormation

AWS CodeBuild

AWS CodeBuild は、コードを構築およびテストするためのサービスです。CodeBuild を使用すると、独自のビルドサーバーをプロビジョニング、管理、スケーリングする必要がなくなり、一般的なプログラミング言語やビルドツール用にパッケージ化されたビルド環境が提供されます。GitLab への接続で CodeBuild を使用する方法の詳細については、AWS CodeBuild 「 ユーザーガイド」のGitLab 接続」を参照してください。

AWS CodePipeline

CodePipeline は、ソフトウェアをリリースするために必要な手順のモデル化、視覚化、および自動化に使用できる継続的な配信サービスです。接続を使用して、CodePipeline ソースアクションのサードパーティーリポジトリを設定できます。

詳細はこちら:

- `SourceConnections` アクションについては、CodePipeline アクション設定のリファレンスページを参照してください。設定パラメータと JSON/YAML スニペット例を表示する場合は、AWS CodePipeline ユーザーガイドの「CodeStarSourceConnection」を参照してください。
- サードパーティーのソースリポジトリを使用してパイプラインを作成する「開始方法」チュートリアルを表示するには、「接続の使用開始」を参照してください。

Service Catalog

Service Catalog を使用すると、組織は での使用が承認された製品のカタログを作成および管理できます AWS。

AWS アカウント と GitHub、GitHub Enterprise、Bitbucket などの外部リポジトリプロバイダー間の接続を承認すると、接続により、Service Catalog 製品をサードパーティーリポジトリを介して管理されるテンプレートファイルに同期できます。

詳細については、「Service Catalog ユーザーガイド」の「Service Catalog 製品を GitHub、GitHub Enterprise、または Bitbucket のテンプレートファイルに同期する」を参照してください。

AWS Proton

AWS Proton は、クラウドインフラストラクチャにデプロイするためのクラウドベースのサービスです。接続を使用して、 AWS Protonのテンプレートのリソース用のサードパーティーリポジトリへのリンクを作成できます。詳細については、AWS Proton ユーザーガイドの「リポジトリのリンクを作成する」を参照してください。

接続のセットアップ

このセクションのタスクを完了して、デベロッパーツールコンソールで接続機能の作成と使用するためのセットアップを行います。

トピック

- にサインアップする AWS
- 接続を作成するアクセス許可を持つポリシーの作成と適用

にサインアップする AWS

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、電話またはテキストメッセージを受け取り、電話キーパッドで検証コードを入力します。

   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。セキュリティベストプラクティスとして、ユーザーに管理アクセス権を割り当て、ルートユーザーアクセスが必要なタスクの実行にはルートユーザーのみを使用するようにしてください。

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、 を保護し 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「アクセス許可セットを作成する」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「グループを追加する」を参照してください。

接続を作成するアクセス許可を持つポリシーの作成と適用

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/ 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。

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

```
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "codeconnections:CreateConnection",
                "codeconnections:DeleteConnection",
                "codeconnections:GetConnection",
                "codeconnections:ListConnections",
                "codeconnections:GetInstallationUrl",
                "codeconnections:GetIndividualAccessToken",
                "codeconnections:ListInstallationTargets",
                "codeconnections:StartOAuthHandshake",
                "codeconnections:UpdateConnectionInstallation",
                "codeconnections:UseConnection"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

6. 次へ を選択します。

> **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、[ビジュアル] 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ビジュアル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. ポリシーを作成 をクリックして、新しいポリシーを保存します。

接続の使用開始

接続を開始する最も簡単な方法は、サードパーティーのソースリポジトリを AWS リソースに関連付ける接続を設定することです。パイプラインを CodeCommit などの AWS ソースに接続する場合

は、ソースアクションとしてパイプラインに接続します。ただし、外部リポジトリがある場合は、接続を作成して、リポジトリをパイプラインに関連付ける必要があります。このチュートリアルでは、Bitbucket リポジトリと自分のパイプラインとの接続を設定します。

このセクションでは、接続を使用します。

- AWS CodePipeline: これらのステップでは、パイプラインソースとして Bitbucket リポジトリを使用してパイプラインを作成します。
- Amazon CodeGuru Reviewer: 次に、Bitbucket リポジトリを CodeGuru Reviewer のフィードバックおよび分析ツールに関連付けます。

トピック

前提条件

開始する前に、「セットアップ」のステップを完了します。また、 AWS サービスに接続し、接続が認証を管理できるようにするサードパーティーのソースリポジトリも必要です。たとえば、Bitbucket リポジトリをソースリポジトリと統合する AWS サービスに接続するとします。

- Bitbucket アカウントを使用して Bitbucket リポジトリを作成します。
- Bitbucket 認証情報を準備します。を使用して接続 AWS マネジメントコンソール を設定すると、Bitbucket 認証情報でサインインするように求められます。

ステップ 1: ソースファイルを編集する

Bitbucket リポジトリを作成すると、デフォルトの `README.md` ファイルが含まれます。このファイルを編集します。

1. Bitbucket リポジトリにログインし、[Source] (送信元) を選択します。
2. `README.md` ファイルを選択し、次にページの上部の [Edit] (編集) を選択します。既存のテキストを削除し、次のテキストを追加します。

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

3. [Commit] (コミット) を選択します。

   README.md ファイルがリポジトリのルートレベルにあることを確認してください。

ステップ 2: パイプラインを作成する

このセクションでは、次のアクションを使用してパイプラインを作成します。

- Bitbucket リポジトリとアクションへの接続を持つソースステージ。
- ビルドアクションを含む AWS CodeBuild ビルドステージ。

ウィザードを使用してパイプラインを作成するには

1. CodePipeline コンソール (http://console.aws.amazon.com/codesuite/codepipeline/home) にサインインします。
2. [ようこそ] ページ、[開始方法] ページ、または [パイプライン] ページで、[パイプラインの作成] を選択します。
3. [ステップ 1: パイプラインの設定を選択する] の [パイプライン名] に「**MyBitbucketPipeline**」と入力します。
4. [サービスロール] で、[New service role (新しいサービスロール)] を選択します。

   > **Note**
   >
   > 既存の CodePipeline サービスロールを代わりに使用する場合は、サービスロールポリシーに対する codeconnections:UseConnection IAM アクセス許可を追加したことを確認してください。CodePipeline サービスロールの手順については、「Add permissions to the the CodePipeline service role」を参照してください。

5. [詳細設定] では、デフォルト値のままにします。アーティファクトストアで、[Default location] (デフォルトの場所)を選択し、パイプライン用に選択したリージョン内のパイプラインのデフォルトのアーティファクトストア (デフォルトとして指定された Amazon S3 アーティファクトバケットなど) を使用します。

> **Note**
>
> これはソースコードのソースバケットではありません。パイプラインのアーティファクトストアです。パイプラインごとに S3 バケットなどの個別のアーティファクトストアが必要です。

[次へ] を選択します。

6. ステップ2：[Add source stage] (ソースステージの追加) ページで、ソースステージを追加します。

   a. [Source provider] (ソースプロバイダー) で、[Bitbucket] を選択します。

   b. [Connection] (接続) で、[Connect to Bitbucket (Bitbucket に接続) を選択します。

   c. [Connect to Bitbucket] (Bitbucket に接続) ページの [Connection name] (接続名) に、作成する接続の名前を入力します。この名前は、後でこの接続を識別するのに役立ちます。

      [Bitbucket apps] (Bitbucket アプリ) で、[Install a new app(新しいアプリをインストールする) を選択します。

   d. アプリのインストールページで、 AWS CodeStar アプリが Bitbucket アカウントに接続しようとしていることを示すメッセージが表示されます。[アクセス権の付与] を選択します。接続を承認すると、Bitbucket 上のリポジトリが検出され、 AWS リソースに関連付けることができます。

   e. 新規インストールの接続 ID が表示されます。[Complete connection (接続の完了)] を選択します。CodePipeline コンソールに戻ります。

   f. [リポジトリ名] で、Bitbucket リポジトリの名前を選択します。

   g. ブランチ名で、リポジトリのブランチを選択します。

   h. [ソースコードの変更時にパイプラインを開始する] オプションが選択されていることを確認します。

   i. [出力アーティファクト形式] で、次の [CodePipeline デフォルト] のいずれかを選択します。

      - [CodePipeline デフォルト] を選択して、パイプライン内のアーティファクトにデフォルトの zip 形式を使用します。
      - [完全クローン] を選択して、パイプライン内のアーティファクトのリポジトリに関する Git メタデータを含めます。これは、CodeBuild アクションでのみサポートされます。

[次へ] を選択します。

7. [Add build stage (ビルドステージの追加)] で、ビルドステージを追加します。

   a. [ビルドプロバイダ] で、[AWS CodeBuild] を選択します。[リージョン] をデフォルトでパイプラインのリージョンにすることを許可します。

   b. [プロジェクトを作成] を選択します。

   c. [プロジェクト名] に、このビルドプロジェクトの名前を入力します。

   d. [環境イメージ] で、[Managed image (マネージド型イメージ)] を選択します。[Operating system] で、[Ubuntu] を選択します。

   e. [ランタイム] で、[Standard (標準)] を選択します。[イメージ] で、[aws/codebuild/standard:5.0] を選択します。

   f. [サービスロール] で、[New service role (新しいサービスロール)] を選択します。

   g. [Buildspec] の Build specifications (ビルド仕様) で、[Insert build commands] (ビルドコマンドの挿入) を選択します。Switch to editor([1]エディタに切り替え)を選択し、Build commands (ビルドコマンド)に以下を貼り付けます。

```
version: 0.2

phases:
  install:
    #If you use the Ubuntu standard image 2.0 or later, you must specify
 runtime-versions.
    #If you specify runtime-versions and use an image other than Ubuntu
 standard image 2.0, the build fails.
    runtime-versions:
      nodejs: 12
      # name: version
    #commands:
      # - command
      # - command
  pre_build:
    commands:
      - ls -lt
      - cat README.md
  # build:
    #commands:
      # - command
      # - command
```

```
  #post_build:
    #commands:
      # - command
      # - command
#artifacts:
  #files:
    # - location
    # - location
  #name: $(date +%Y-%m-%d)
  #discard-paths: yes
  #base-directory: location
#cache:
  #paths:
    # - paths
```

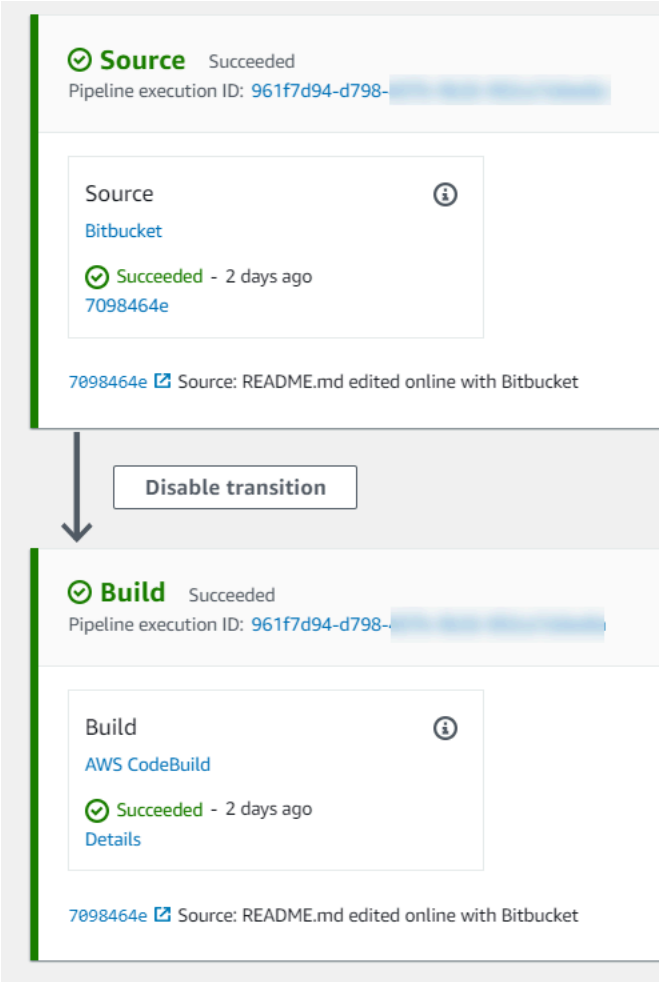
h. [Continue to CodePipeline] (CodePipeline に進む) を選択します。CodePipeline コンソールに戻り、ビルドコマンドを使用して設定する CodeBuild プロジェクトが作成されます。ビルドプロジェクトでは、サービスロールを使用して AWS サービスのアクセス許可を管理します。このステップには数分かかる場合があります。

i. [次へ] を選択します。

8. [Step 4: Add deploy stage (ステップ 4: デプロイステージの追加)] ページで、[Skip deploy stage (デプロイステージのスキップ)] を選択し、[スキップ] を選択して警告メッセージを受け入れます。[次へ] を選択します。

9. [Step 5: Review (ステップ 5: 確認)] で、[パイプラインの作成] を選択します。

10. パイプラインが正常に作成されると、パイプラインが実行されます。



11. ビルドが成功した段階で、[詳細]を選択します。

    [実行の詳細] で、CodeBuild ビルド出力を表示します。README.md ファイルの内容は、コマンドで次のように出力されます。

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

```
35 [Container] 2020/06/05 19:14:51 Running command cat README.md
36 This is a Bitbucket repository!
37 [Container] 2020/06/05 19:14:51 Phase complete: PRE_BUILD State: SUCCEEDED
38 [Container] 2020/06/05 19:14:51 Phase context status code:  Message:
39 [Container] 2020/06/05 19:14:51 Entering phase BUILD
40 [Container] 2020/06/05 19:14:51 Phase complete: BUILD State: SUCCEEDED
41 [Container] 2020/06/05 19:14:51 Phase context status code:  Message:
42 [Container] 2020/06/05 19:14:51 Entering phase POST_BUILD
43 [Container] 2020/06/05 19:14:51 Phase complete: POST_BUILD State: SUCCEEDED
44 [Container] 2020/06/05 19:14:51 Phase context status code:  Message:
```

ステップ 3: リポジトリを CodeGuru Reviewer に関連付ける

接続を作成したら、その接続を同じアカウントのすべての AWS リソースに使用できます。例えば、パイプラインの CodePipeline ソースアクションと CodeGuru Reviewer のリポジトリコミット分析に同じ Bitbucket 接続を使用できます。

1. CodeGuru Reviewer コンソールにサインインします。
2. CodeGuru Reviewerで、[リポジトリの関連付け]を選択します。

   1 ページのウィザードが開きます。
3. [Select source provider] (ソースプロバイダーの選択) で、[Bitbucket] を選択します。
4. Bitbucket に接続する (AWS CodeConnections を使用) で、パイプライン用に作成した接続を選択します。
5. [Repository location] (リポジトリの場所) で、Bitbucket リポジトリの名前を選択し、Associate (関連付け) を選択します 。

   コードレビューの設定を続行できます。詳細については、Amazon CodeGuru Reviewer User Guide の「Amazon CodeGuru Reviewer User Guide」を参照してください。

接続の使用

接続は、 AWS リソースを外部コードリポジトリに接続するために使用する構成です。各接続は、Bitbucket などのサードパーティーリポジトリに接続 AWS CodePipeline するために などのサービスに付与できるリソースです。例えば、CodePipeline で接続を追加して、サードパーティーのコードリポジトリでコードが変更されたときにパイプラインをトリガーできるようになります。AWS リソースを GitHub Enterprise Server などのインストール済みプロバイダータイプに接続することもできます。

> **Note**
>
> GitHub または GitHub Enterprise Server の組織の場合、GitHub アプリを複数の GitHub Organizations にインストールすることはできません。アプリから GitHub Organization へのマッピングは 1:1 マッピングです。1 つの組織では一度に 1 つのアプリしか持つことができませんが、同じアプリを指す複数の接続を持つことができます。詳細については、「AWS CodeConnections の接続が組織と連携する方法」を参照してください。

インストール済みプロバイダータイプ (GitHub Enterprise Server など) への接続を作成する場合、コンソールがホストを作成します。ホストは、プロバイダがインストールされているサーバーを表すために作成するリソースです。詳細については、「ホストの使用」を参照してください。

接続を作成するときは、 コンソールのウィザードを使用して接続アプリをサードパーティープロバイダーにインストールし、新しい接続に関連付けます。 アプリをインストール済みである場合は、それを使用できます。

> **Note**
>
> 欧州 (ミラノ) で接続を使用するには AWS リージョン、以下を行う必要があります。
>
> 1. リージョン固有のアプリをインストールする
> 2. リージョンを有効にする
>
> このリージョン固有のアプリで、欧州 (ミラノ) リージョンの接続をサポートします。サードパーティープロバイダーのサイトで公開されているアプリであり、他のリージョンの接続をサポートする既存のアプリとは別のものです。このアプリをインストールすることで、このリージョンでのみサービスとデータを共有することをサードパーティープロバイダーに許可します。アプリをアンインストールすることでいつでもアクセス許可を取り消すことができます。
> リージョンを有効にしない限り、サービスはデータを処理または保存しません。このリージョンを有効にすることで、データを処理および保存するアクセス許可をサービスに付与したことになります。
> リージョンが有効になっていなくても、リージョン固有のアプリがインストールされたままであれば、サードパーティープロバイダーはお客様のデータをサービスと共有できます。したがって、リージョンを無効にしたら、必ずアプリをアンインストールしてください。詳細については、「リージョンの有効化」を参照してください。

接続の詳細については、AWS CodeConnections API リファレンスを参照してください。Bitbucket の CodePipeline ソースアクションの詳細については、AWS CodePipeline User Guide の「CodestarConnectionSource」を参照してください。

接続を使用するために必要なアクセス許可を持つポリシーを作成または AWS Identity and Access Management (IAM) ユーザーまたはロールにアタッチするには、「」を参照してくださいAWS CodeConnections アクセス許可リファレンス。CodePipeline サービスロールが作成された日時によっては、support AWS CodeConnections へのアクセス許可を更新する必要がある場合がありま

す。手順については、AWS CodePipeline User Guideの「Update the service role」を参照してください。

トピック

接続を作成する

次のサードパーティーのプロバイダーのタイプへの接続を作成できます。

- Bitbucket への接続を作成するには、「Bitbucket への接続を作成する」を参照してください。
- GitHub または GitHub Enterprise Cloud への接続を作成するには、「GitHub への接続を作成する」を参照してください。
- ホストリソースの作成など、GitHub Enterprise Server への接続を作成するには、「GitHub Enterprise Server への接続を作成する」を参照してください。
- GitLab への接続を作成するには、「GitLab への接続を作成する」を参照してください。
- Azure DevOps への接続を作成するには、「Azure DevOps への接続を作成する」を参照してください。

> **Note**
>
> 2024 年 7 月 1 日以降、コンソールはリソース ARN codeconnectionsに との接続を作成します。両方のサービスプレフィックスを持つリソースは、コンソールに引き続き表示されます。

Azure DevOps への接続を作成する

AWS マネジメントコンソール または AWS Command Line Interface (AWS CLI) を使用して、Azure DevOps でホストされているリポジトリへの接続を作成できます。

開始する前に:

- Azure DevOps でアカウントを作成済みである必要があります。
- Azure DevOps ポータルでプロジェクトと Azure リポジトリを既に作成している必要があります。アカウントには、リポジトリへの管理者アクセス権が必要です。

> **Note**
>
> Azure DevOps リポジトリへの接続を作成できます。Azure Cloud Hosting などのインストール済み (ホスト上) Azure プロバイダータイプはサポートされていません。「AWS CodeConnections でサポートされているプロバイダーとバージョン」を参照してください。

> **Note**
>
> 接続は、接続の作成に使用されたアカウントで所有するリポジトリへのアクセスだけを提供します。

トピック

- Azure DevOps への接続を作成する (コンソール)
- Azure DevOps への接続を作成する (CLI)

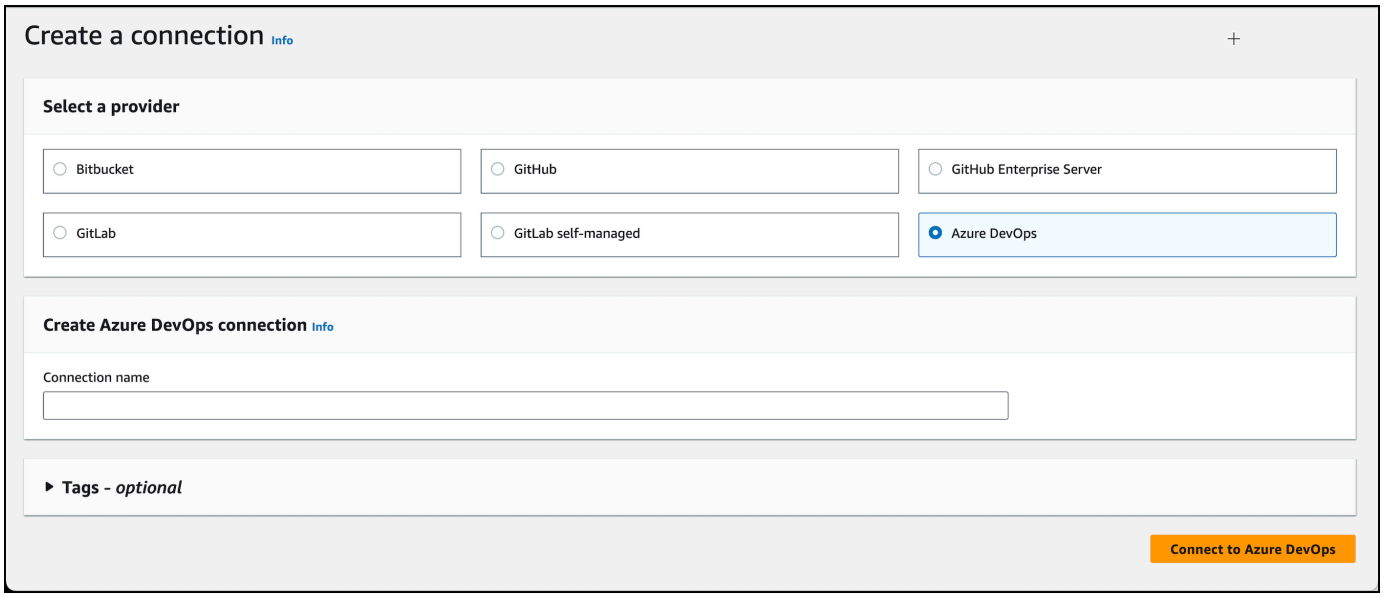
Azure DevOps への接続を作成する (コンソール)

コンソールを使用して、Azure DevOps への接続を作成できます。

> **Note**
>
> 2024 年 7 月 1 日以降、コンソールはリソース ARN codeconnectionsに との接続を作成します。両方のサービスプレフィックスを持つリソースは、コンソールに引き続き表示されます。

ステップ 1: 接続の作成

1. にサインインし AWS マネジメントコンソール、 で AWS 開発者ツールコンソールを開きますhttps://console.aws.amazon.com/codesuite/settings/connections。
2. 選択[設定] > [接続] を選択してから、[接続を作成する。
3. Azure DevOps リポジトリへの接続を作成するには、[プロバイダーを選択する] で、[Azure DevOps] を選択します。[接続名] に、作成する接続の名前を入力します。 [Azure DevOps に接続] を選択して、ステップ 2 に進みます。

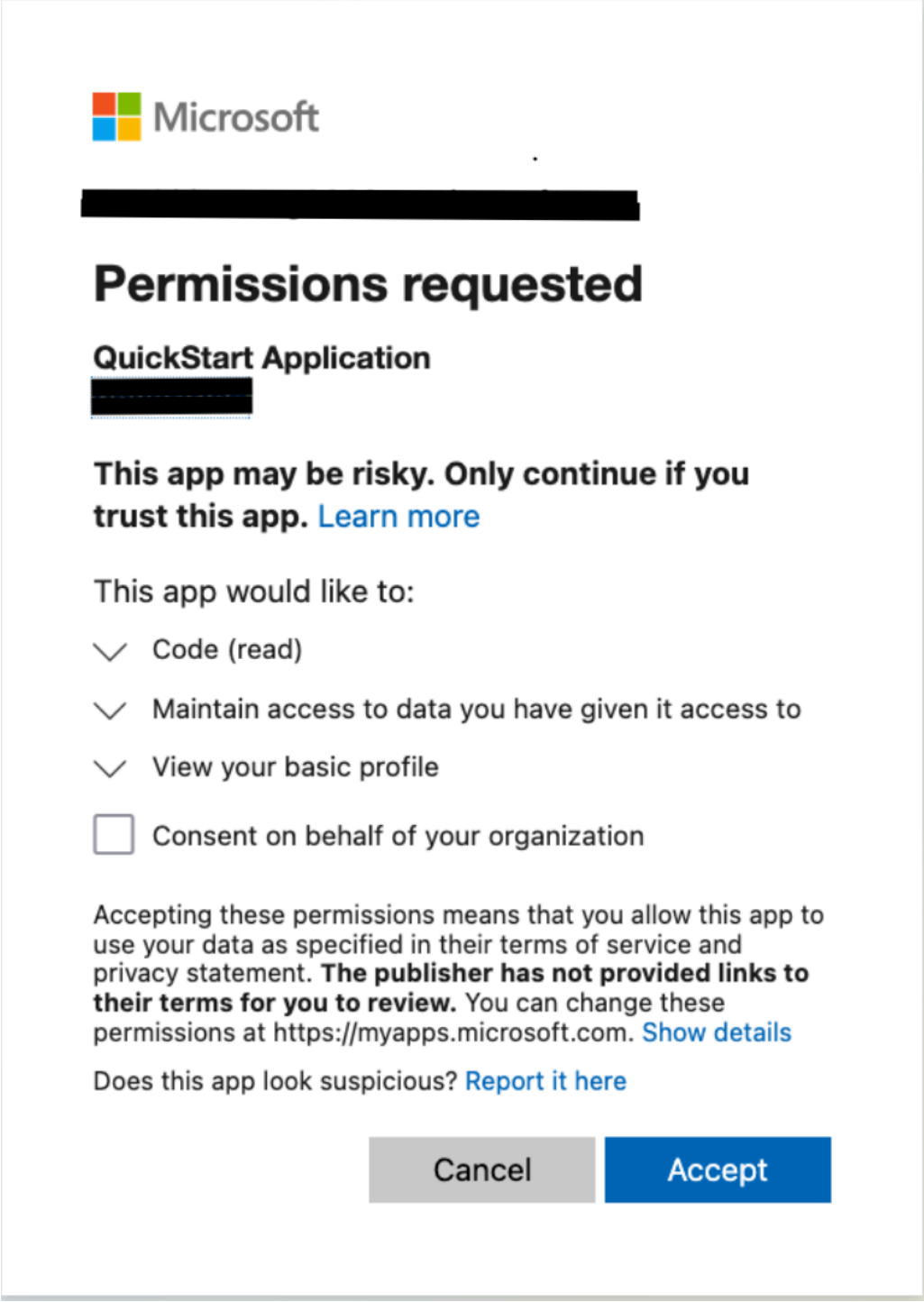


ステップ 2: Azure DevOps に接続する

1. [Azure DevOps に接続] 設定ページに、接続名が表示されます。

2. Microsoft のログインページが表示されたら、認証情報を使用してログインし、続行を選択します。

   Azure DevOps への接続を初めて作成する場合は、アクセス許可を付与する必要がある場合があります AWS マネジメントコンソール。



3. [Accept (承諾)] を選択します。

4. 接続ページで、新規インストールの接続 ID が表示されます。
5. Connect を選択して接続を確立します。作成された接続が接続リストに表示され、使用可能なステータスになり、使用できる状態になります。

Azure DevOps への接続を作成する (CLI)

AWS Command Line Interface (AWS CLI) を使用して接続を作成できます。

これを行うには、create-connection コマンドを使用します。

> **Important**
>
> AWS CLI または を介して作成された接続 AWS CloudFormation は、デフォルトで PENDINGステータスです。CLI または との接続を作成したら CloudFormation、コンソールを使用して接続を編集し、ステータスを にしますAVAILABLE。

Azure DevOps への接続を作成するには

1. ターミナル (Linux/macOS/Unix) またはコマンドプロンプト (Windows) を開きます。 AWS CLI を使用して create-connection コマンドを実行し、接続--connection-nameの --provider-typeと を指定します。この例では、サードパーティープロバイダー名は AzureDevOps で、指定された接続名は MyConnection です。

   ```
   aws codeconnections create-connection --provider-type AzureDevOps --connection-name
    MyConnection
   ```

   成功した場合、このコマンドは次のような接続 ARN 情報を返します。

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

2. コンソールを使用して接続を完了します。詳細については、「保留中の接続の更新」を参照してください。

Bitbucket への接続を作成する

AWS マネジメントコンソール または AWS Command Line Interface (AWS CLI) を使用して、bitbucket.org でホストされているリポジトリへの接続を作成できます。

開始する前に:

- Bitbucket で、アカウントを作成しておく必要があります。
- bitbucket.org で、コードリポジトリを作成しておく必要があります。

> **Note**
>
> Bitbucket Cloudリポジトリへの接続を作成できます。Bitbucket サーバーなど、インストールされている Bitbucket プロバイダーのタイプはサポートされていません。「AWS CodeConnections でサポートされているプロバイダーとバージョン」を参照してください。

> **Note**
>
> 接続は、接続の作成に使用されたアカウントで所有するリポジトリへのアクセスだけを提供します。
> アプリケーションを Bitbucket ワークスペースにインストールする場合は、「ワークスペースを管理する」アクセス許可が必要です。アクセス許可がないと、アプリケーションをインストールするオプションは表示されません。

トピック

- Bitbucket (コンソール) への接続を作成する
- Bitbucket (CLI) への接続を作成する

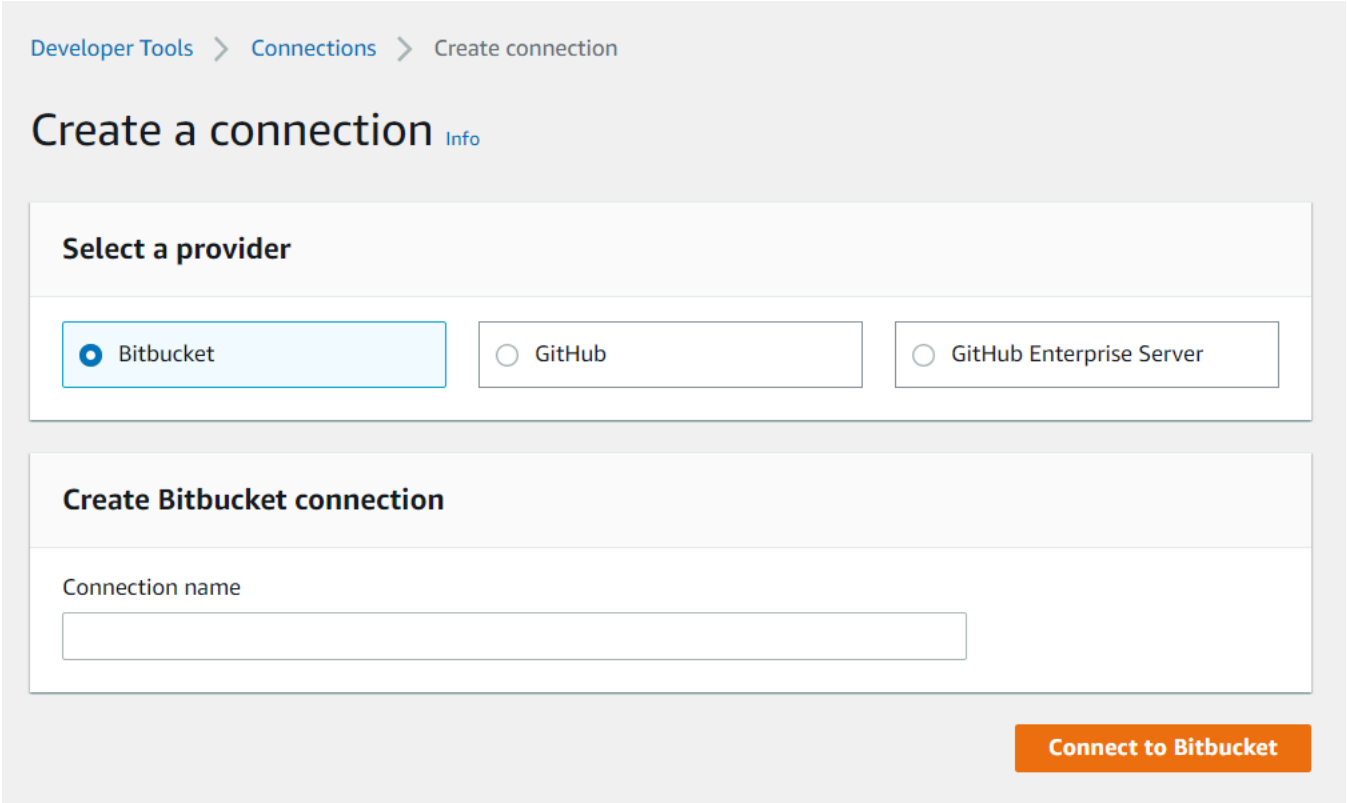
Bitbucket (コンソール) への接続を作成する

コンソールを使用して Bitbucket への接続を作成できます。

> **Note**
>
> 2024 年 7 月 1 日以降、コンソールはリソース ARN codeconnectionsに との接続を作成します。両方のサービスプレフィックスを持つリソースは、コンソールに引き続き表示されます。

ステップ 1: 接続の作成

1. にサインインし AWS マネジメントコンソール、 で AWS 開発者ツールコンソールを開きますhttps://console.aws.amazon.com/codesuite/settings/connections。
2. 選択[設定] > [接続] を選択してから、[接続を作成する。
3. Bitbucket リポジトリへの接続を作成するには、Select a provider] (プロバイダーを選択する) で、[Bitbucket] を選択します。[接続名] に、作成する接続の名前を入力します。[Connect to Bitbucket] (Bitbucket に接続) を選択し、ステップ 2 に進みます。

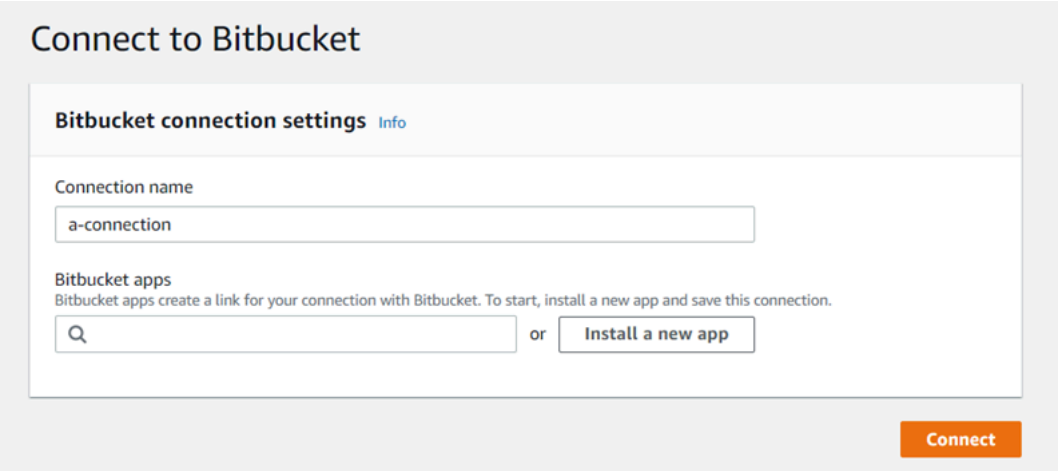


ステップ 2: Bitbucket に接続する

1. [Connect to Bitbucket] 設定ページに、接続名が表示されます。

[Bitbucket apps] (Bitbucket アプリ) で、アプリのインストールを選択するか、アプリを作成するために [Install a new app] (新しいアプリをインストールする) を選択します。

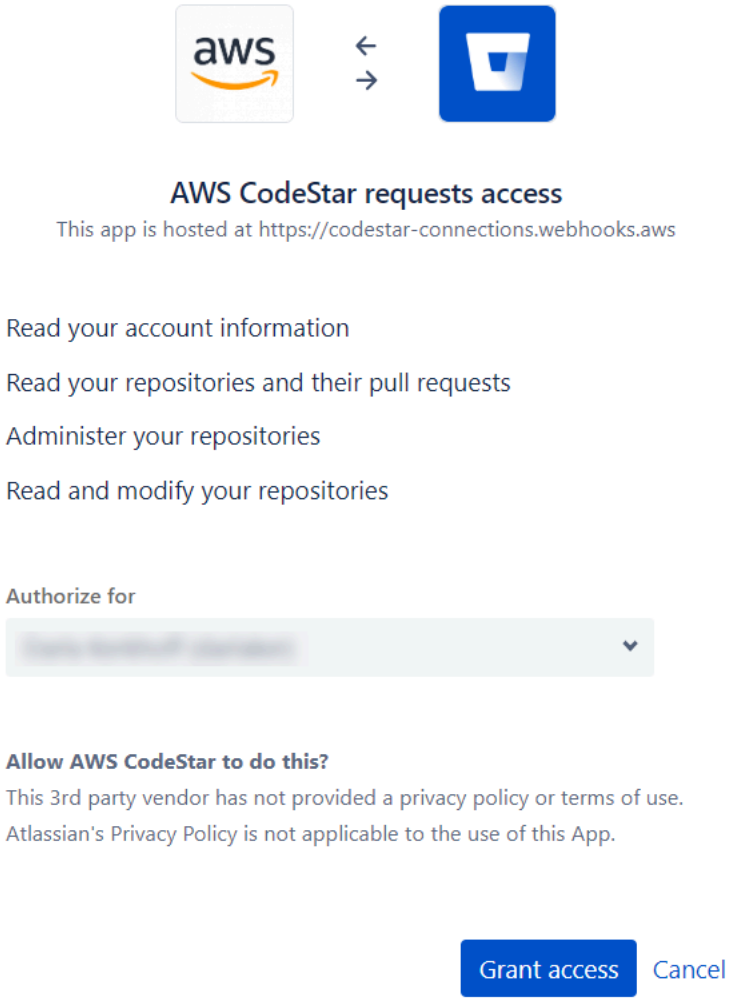
> **Note**
>
> アプリケーションは、Bitbucket ワークスペースまたはアカウントごとに 1 回だけインストールします。Bitbucket アプリを既にインストールしている場合は、それを選択してこのセクションの最後のステップに移動します。



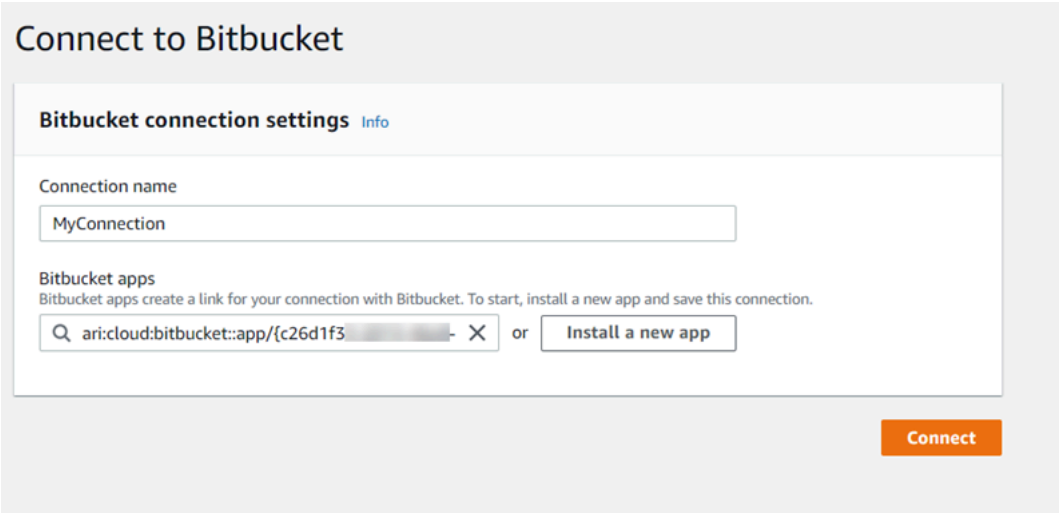
2. Bitbucket のログインページが表示されたら、認証情報を使用してログインし、続行を選択します。
3. アプリのインストールページで、 AWS CodeStar アプリが Bitbucket アカウントに接続しようとしていることを示すメッセージが表示されます。

   Bitbucket ワークスペースを使用している場合は、[Authorize for] (承認対象) オプションをそのワークスペースに変更します。管理者権限のあるワークスペースのみが表示されます。

   [アクセス権の付与] を選択します。



4. Bitbucketアプリには、新規インストールの接続 ID が表示されます。接続 を選択します。作成された接続が接続リストに表示されます。



Bitbucket (CLI) への接続を作成する

AWS Command Line Interface (AWS CLI) を使用して接続を作成できます。

これを行うには、create-connection コマンドを使用します。

> **Important**
>
> AWS CLI または を介して作成された接続 AWS CloudFormation は、デフォルトで PENDINGステータスです。CLI または との接続を作成したら CloudFormation、コンソールを使用して接続を編集し、ステータスを にしますAVAILABLE。

Bitbucket への接続を作成するには

1. ターミナル (Linux/macOS/Unix) またはコマンドプロンプト (Windows) を開きます。 AWS CLI を使用して create-connection コマンドを実行し、接続--connection-nameの --provider-typeと を指定します。この例では、サードパーティープロバイダー名は Bitbucket で、指定された接続名は MyConnection です。

   ```
   aws codeconnections create-connection --provider-type Bitbucket --connection-name
    MyConnection
   ```

   成功した場合、このコマンドは次のような接続 ARN 情報を返します。

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

2. コンソールを使用して接続を完了します。詳細については、「保留中の接続の更新」を参照してください。

GitHub への接続を作成する

AWS マネジメントコンソール または AWS Command Line Interface (AWS CLI) を使用して、GitHub への接続を作成できます。

開始する前に:

- GitHub でアカウントを作成しておく必要があります。
- サードパーティーのコードリポジトリを予め作成しておく必要があります。

> **Note**
>
> 接続を作成するには、GitHub 組織の所有者である必要があります。組織のリポジトリでない場合、ユーザーがリポジトリの所有者である必要があります。

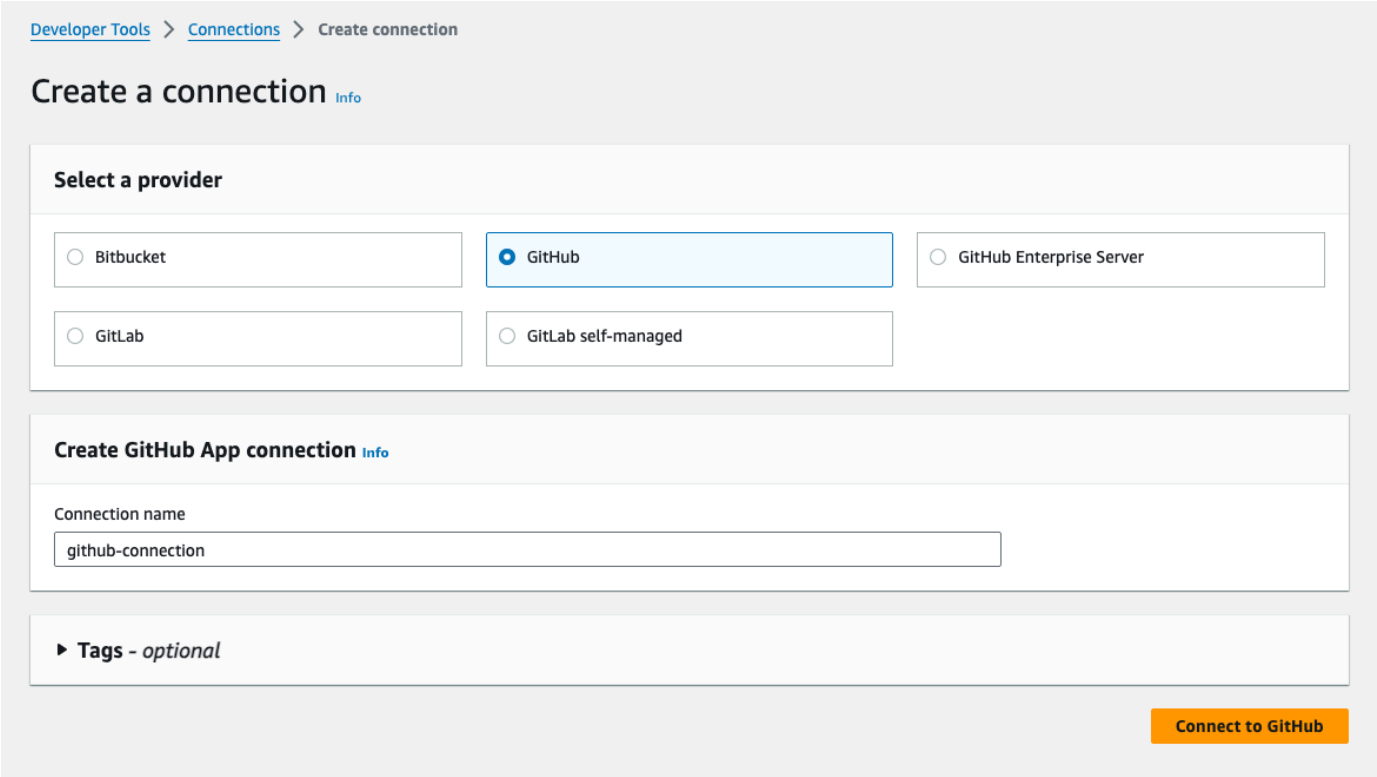
トピック

GitHub (コンソール) への接続を作成する

コンソールを使用して、GitHub への接続を作成できます。

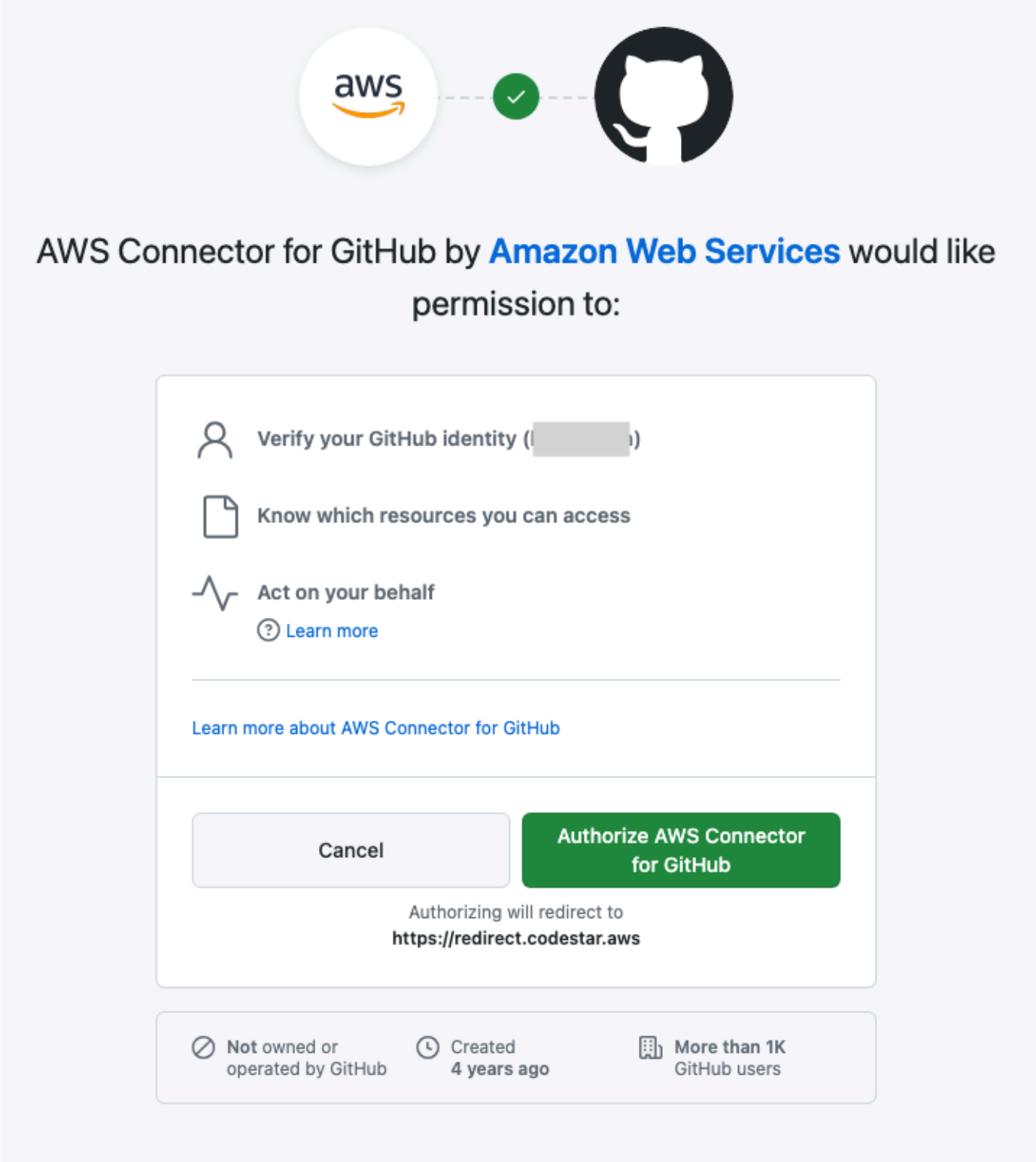
> **Note**
>
> 2024 年 7 月 1 日以降、コンソールはリソース ARN `codeconnections`に との接続を作成します。両方のサービスプレフィックスを持つリソースは、コンソールに引き続き表示されます。

1. にサインインし AWS マネジメントコンソール、 で開発者ツールコンソールを開きますhttps://console.aws.amazon.com/codesuite/settings/connections。
2. 選択[設定] > [接続] を選択してから、[接続を作成する。
3. GitHub または GitHub Enterprise Cloud リポジトリへの接続を作成するには、[Select a provider] (プロバイダの選択) で、[GitHub] を選択します。[接続名] に、作成する接続の名前を入力します。 [Connect to GitHub] (GitHubに接続) を選択して、ステップ 2 に進みます。

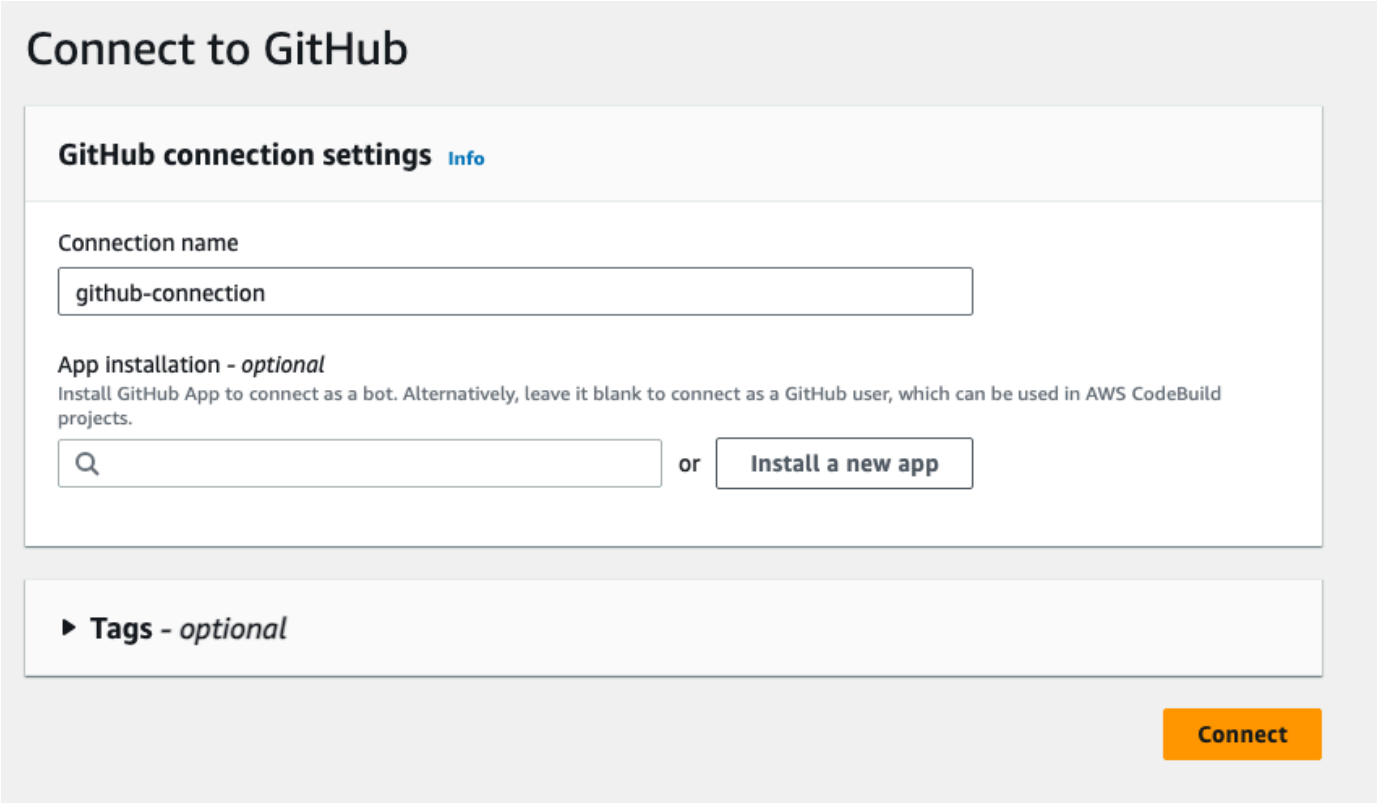


GitHub への接続を作成するには

1. [GitHub connection settings] で、[Connection name] に接続名が表示されます。[Connect to GitHub] (GitHub に接続) を選択します。アクセス要求のページが表示されます。



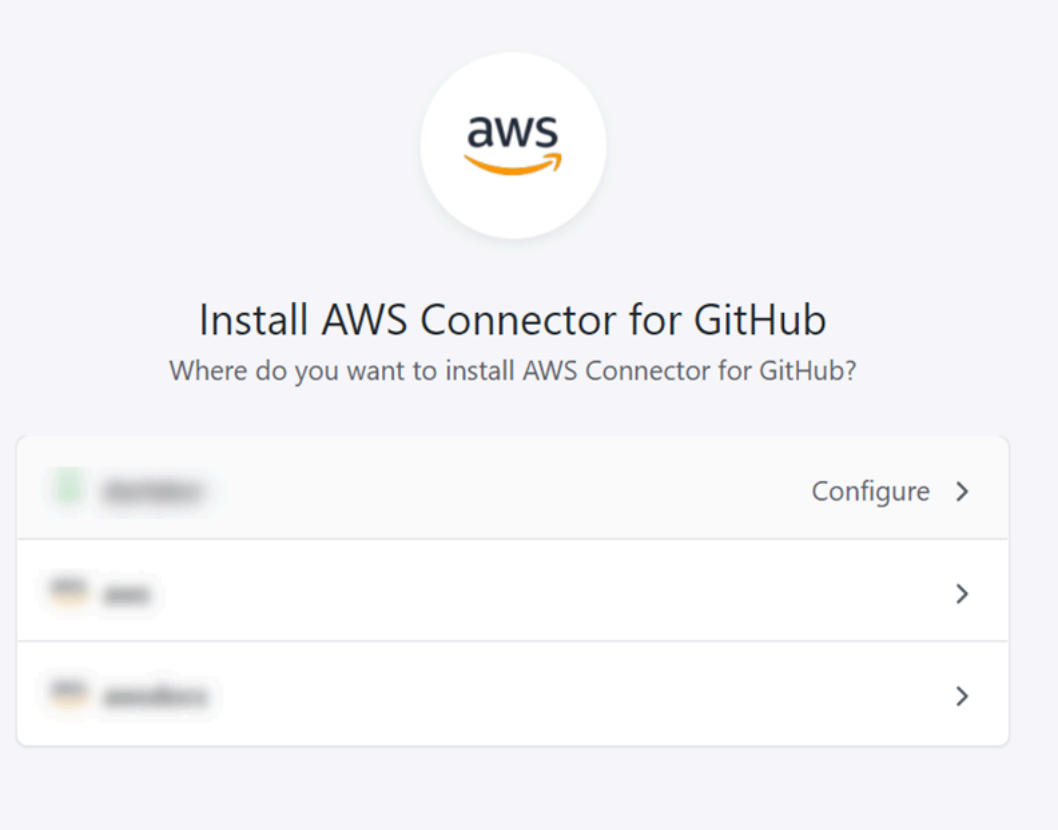
2. GitHub の AWS コネクタの承認を選択します。接続ページには [GitHub Apps] フィールドが表示されます。



3. [GitHub Apps] (Bitbucket アプリ) で、アプリのインストールを選択するか、[Install a new app] (新しいアプリをインストールする) を選択してアプリを作成します。

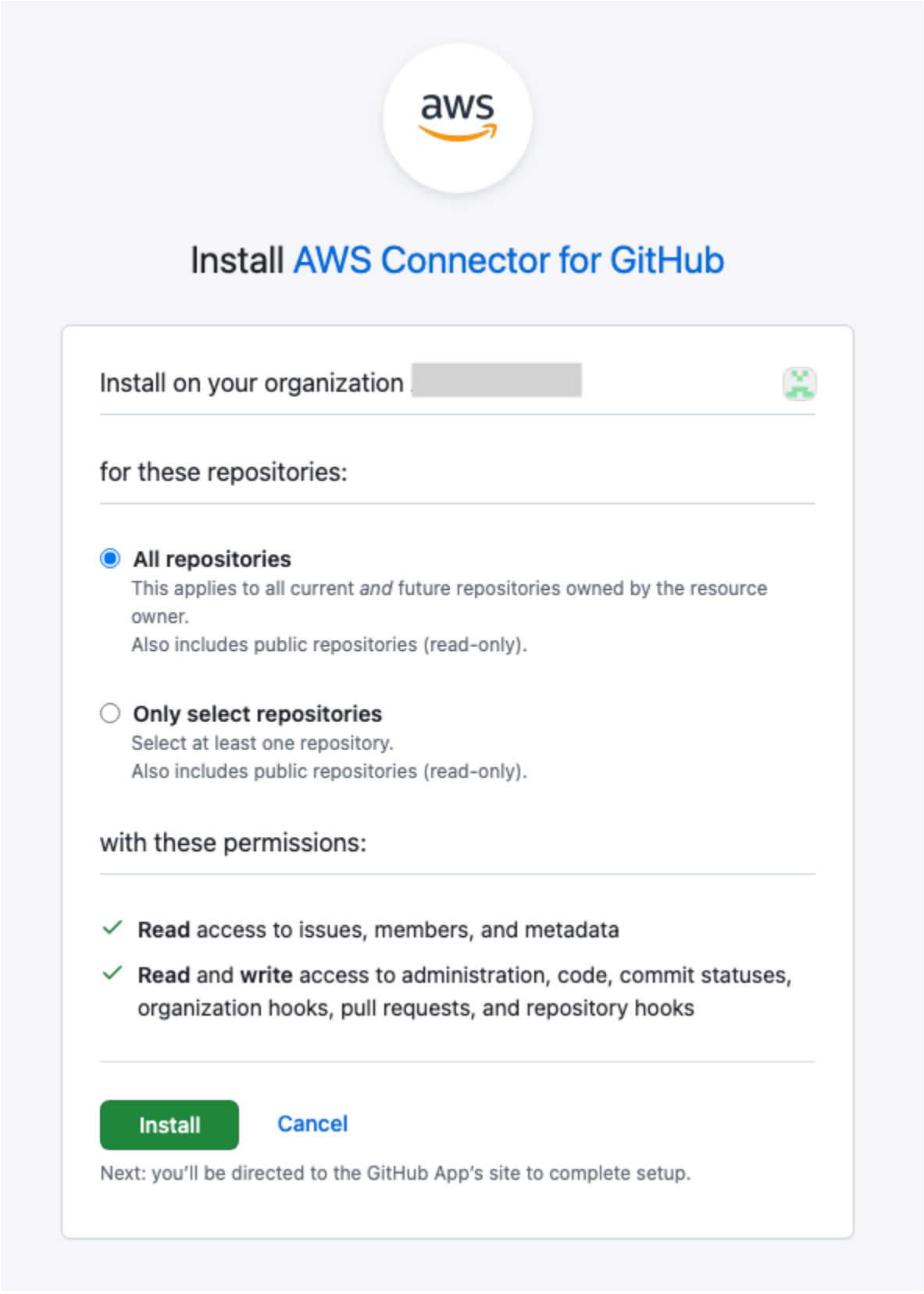
> **Note**
>
> 特定のプロバイダーへのすべての接続に対してアプリを 1 つインストールします。AWS Connector for GitHub アプリを既にインストールしている場合は、それを選択してこのステップをスキップします。

4. 「AWS Connector for GitHub をインストール」ページで、アプリケーションをインストールするアカウントを選択します。



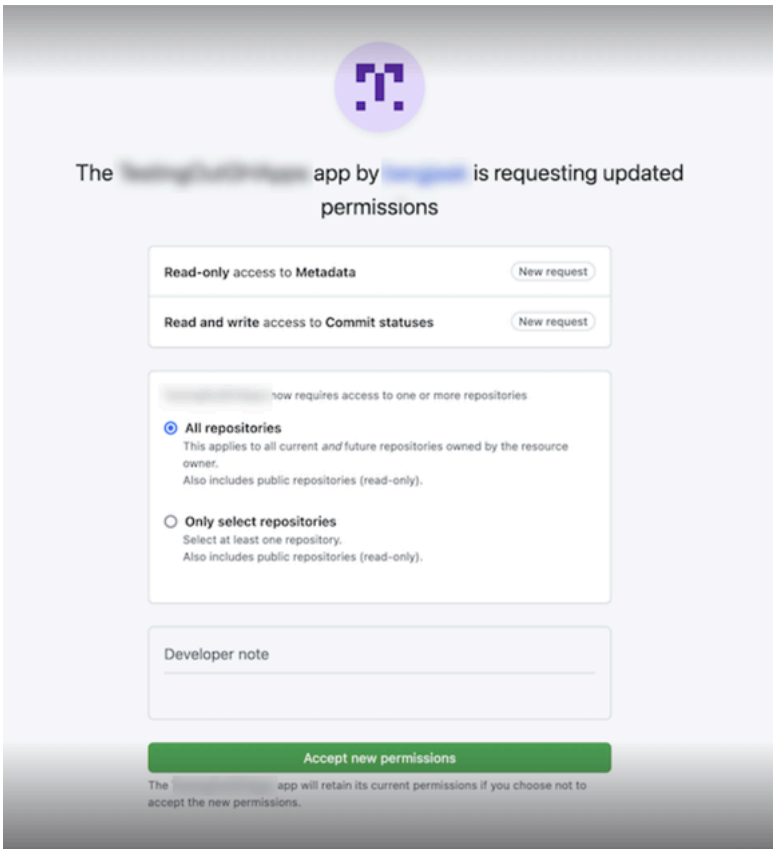
> **Note**
>
> アプリは、GitHub アカウントごとに 1 回だけインストールします。アプリをインストール済みである場合は、Configure (設定) をクリックしてアプリのインストールの変更ページに進むか、戻るボタンでコンソールに戻ることができます。

5. 「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。



このステップの後、更新された権限ページが GitHub に表示されることがあります。

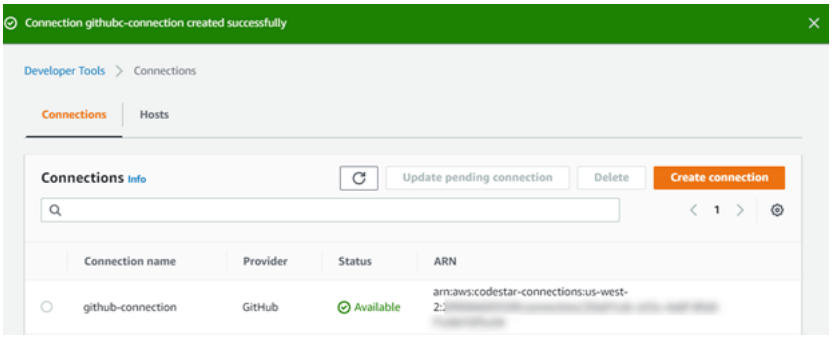
6. AWS Connector for GitHub アプリの権限が更新されたことを示すページが表示されたら、[Accept new permissions] (新しい権限を承認) を選択します。



7. 「Connect to GitHub」(GitHub へ接続) ページに戻ります。新規インストールの接続 ID が [GitHub Apps] (GitHub アプリ) に表示されます。接続 を選択します。

作成した接続を表示する

- 作成された接続が接続リストに表示されます。



GitHub (CLI) への接続を作成する

AWS Command Line Interface (AWS CLI) を使用して GitHub への接続を作成できます。

これを行うには、create-connection コマンドを使用します。

> **Important**
>
> AWS CLI または を介して作成された接続 AWS CloudFormation は、デフォルトで PENDINGステータスです。CLI または との接続を作成したら CloudFormation、コンソールを使用して接続を編集し、ステータスを にしますAVAILABLE。

GitHub への接続を作成するには

1. ターミナル (Linux/macOS/Unix) またはコマンドプロンプト (Windows) を開きます。 AWS CLI を使用して create-connection コマンドを実行し、接続--connection-nameの --provider-typeと を指定します。この例では、サードパーティープロバイダー名は GitHub で、指定された接続名は MyConnection です。

   ```
   aws codeconnections create-connection --provider-type GitHub --connection-name
    MyConnection
   ```

   成功した場合、このコマンドは次のような接続 ARN 情報を返します。

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

2. コンソールを使用して接続を完了します。詳細については、「保留中の接続の更新」を参照してください。

GitHub Enterprise Server への接続を作成する

接続を使用して、 AWS リソースをサードパーティーリポジトリに関連付けます。 AWS マネジメントコンソール または AWS Command Line Interface (AWS CLI) を使用して、GitHub Enterprise Server への接続を作成できます。

接続は、接続の作成時に GitHub アプリのインストールを承認するために使用される GitHub Enterprise Server アカウントが所有するリポジトリにだけアクセスを提供します。

開始する前に:

- GitHub Enterprise Server インスタンスとリポジトリが必要です。
- GitHub アプリを作成し、このセクションで説明するホストリソースを作成するには、GitHub Enterprise Server インスタンスの管理者である必要があります。

> **Important**
>
> GitHub Enterprise Server 用にホストをセットアップすると、Webhook イベントデータ用の VPC エンドポイントが自動的に作成されます。2020 年 11 月 24 日より前にホストを作成し、VPC PrivateLink ウェブフックエンドポイントを使用する場合は、最初にホストを削除してから、新しいホストを作成する必要があります。

> **Note**
>
> GitHub Enterprise Server または GitLab セルフマネージドの組織では、使用可能なホストを渡しません。組織内の接続ごとに新しいホストを作成し、ホストのネットワークフィールド (VPC ID、サブネット IDs、セキュリティグループ IDs) に必ず同じ情報を入力する必要があります。詳細については、「組織をサポートするインストール済みプロバイダーの接続とホストのセットアップ」を参照してください。

トピック

- GitHub Enterprise Server への接続を作成する (コンソール)
- GitHub Enterprise Server への接続を作成する (CLI)

GitHub Enterprise Server への接続を作成する (コンソール)

GitHub Enterprise Server 接続を作成するには、GitHub Enterprise Server のインストール先の情報を提供し、GitHub Enterprise の認証情報で接続の作成を許可します。

> **Note**
>
> 2024 年 7 月 1 日以降、コンソールはリソース ARN codeconnectionsに との接続を作成します。両方のサービスプレフィックスを持つリソースは、コンソールに引き続き表示されます。

トピック

- GitHub Enterprise Server 接続を作成する (コンソール)

GitHub Enterprise Server 接続を作成する (コンソール)

GitHub Enterprise Server への接続を作成するには、サーバーの URL と GitHub Enterprise の認証情報を準備してください。

ホストを作成するには

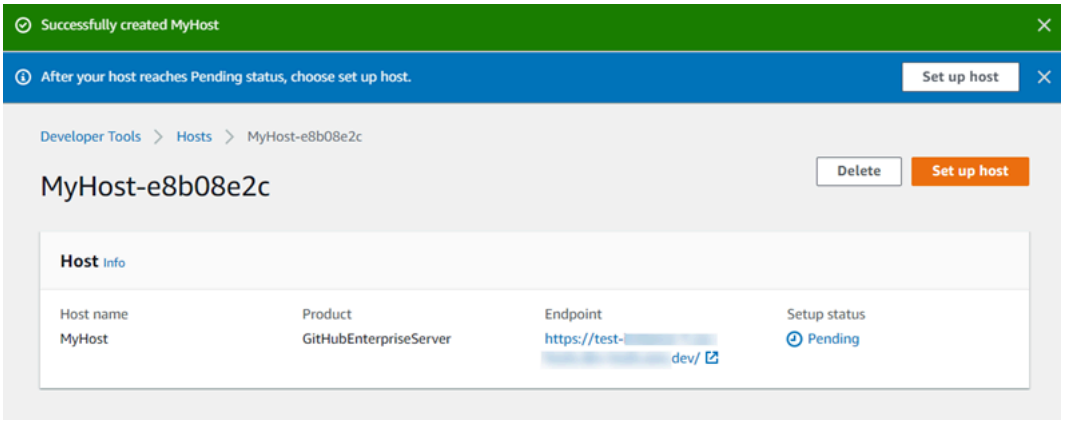
1. にサインインし AWS マネジメントコンソール、 で AWS 開発者ツールコンソールを開きますhttps://console.aws.amazon.com/codesuite/settings/connections。
2. [Hosts (ホスト)]タブで、[Create host (ホストの作成)]を選択します。
3. [ホスト名]に、ホストに使用する名前を入力します。
4. [プロバイダーを選択] で、次のいずれかを選択します。
   - GitHub Enterprise Server
   - GitLab セルフマネージド
5. [URL] に、プロバイダーがインストールされているインフラストラクチャのエンドポイントを入力します。
6. サーバーが Amazon VPC 内に設定されていて、VPC に接続する場合は、 Use a VPC (VPC を使用) を選択します。それ以外の場合、[No VPC] を選択します。
7. Amazon VPC でインスタンスを起動し、VPC に接続する場合は、[Use a VPC] (PC を使用) をクリックして、以下を完了します。
   a. [VPC ID] で、 VPC ID を選択します。インスタンスがインストールされているインフラストラクチャに VPC を選択するか、VPN または Direct Connect を介してインスタンスにアクセスできる VPC を選択します。

b. プライベート VPC を設定していて、非公開認証局を使用して TLS 検証を実行するようにインスタンスを設定している場合は、[TLS 証明書] に証明書 ID を入力します。TLS 証明書の値 は 証明書のパブリックキーです。

8. [Create host] (ホストの作成) を選択します。
9. ホストの詳細ページが表示されたら、ホストの作成に伴ってホストのステータスが変化します。

> **Note**
>
> ホスト設定に VPC 設定が含まれている場合は、ホストネットワークコンポーネントのプロビジョニングに数分間かかります。

ホストのステータスがPending (保留中) になるのを待ってから、セットアップを完了します。詳細については、「保留中のホストをセットアップする」を参照してください。

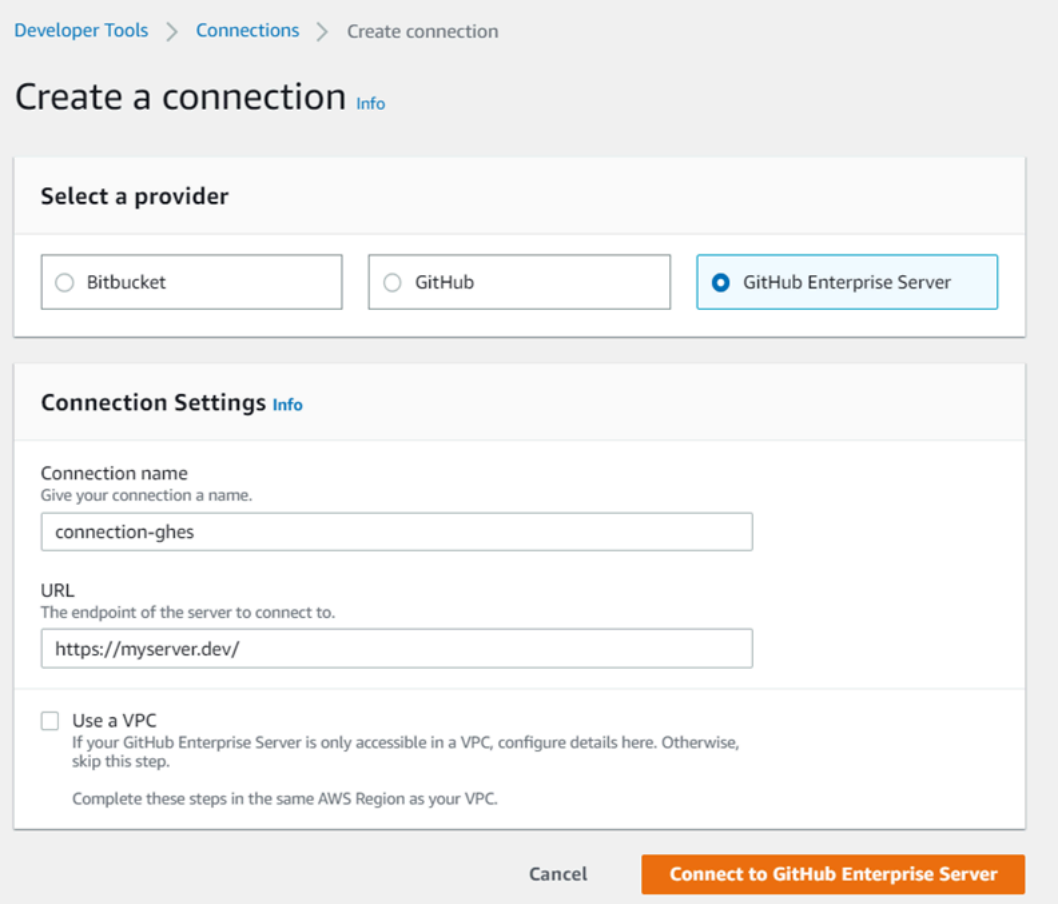


ステップ 2: GitHub Enterprise Server への接続を作成する (コンソール)

1. にサインイン AWS マネジメントコンソール し、 で開発者ツールコンソールを開きますhttps://console.aws.amazon.com/codesuite/settings/connections。
2. 選択[設定] > [接続] を選択してから、[接続を作成する。
3. インストール済みの GitHub Enterprise Server リポジトリへの接続を作成するには、[GitHub Enterprise Server] を選択します。

GitHub Enterprise Server に接続する

1. [Connection name] (接続名) に、接続の名前を入力します。



2. [URL] に、サーバーのエンドポイントを入力します。

> **Note**
>
> 提供された URL がすでに接続用の GitHub Enterprise Server をセットアップするために使用されている場合は、そのエンドポイント用に以前に作成されたホストリソース ARN を選択するように求められます。

3. (オプション) Amazon VPC でサーバーを起動し、VPC に接続する場合は、[VPC を使用] を選択して、以下を完了します。

> **Note**
>
> GitHub Enterprise Server または GitLab セルフマネージドの組織では、使用可能なホストを渡しません。組織内の接続ごとに新しいホストを作成し、ホストのネットワークフィールド (VPC ID、サブネット IDs、セキュリティグループ IDs) に必ず同じ情報を入

力する必要があります。詳細については、「組織をサポートするインストール済みプロバイダーの接続とホストのセットアップ」を参照してください。

a. [VPC ID] で、 VPC ID を選択します。Hub Enterprise Server インスタンスがインストールされているインフラストラクチャに VPC を選択するか、VPN または Direct Connect を介してGitHub Enterprise Server インスタンスにアクセスできる VPC を選択します。

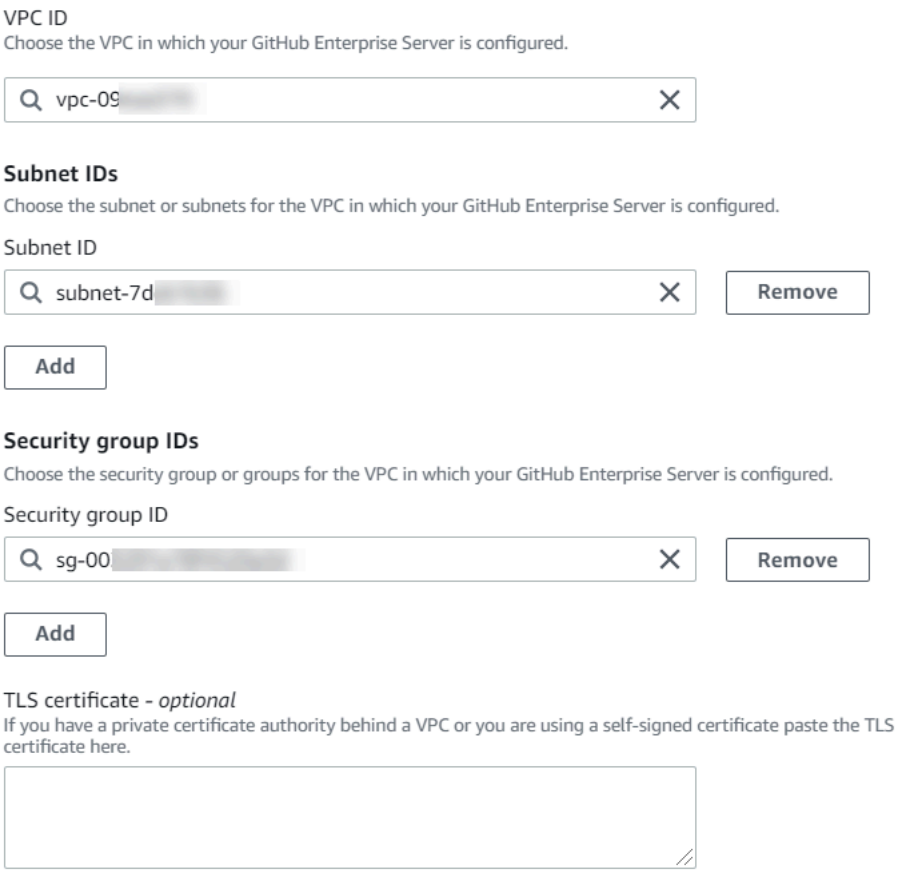
b. [サブネット ID] で、[Add] を選択します。このフィールドで、ホストに使用するサブネット ID を選択します。最大 10 個のサブネットを選択できます。

   GitHub Enterprise Server インスタンスがインストールされているインフラストラクチャのサブネット、または VPN または Direct Connect を介してインストールされた GitHub Enterprise Server インスタンスにアクセスできるサブネットを選択してください。

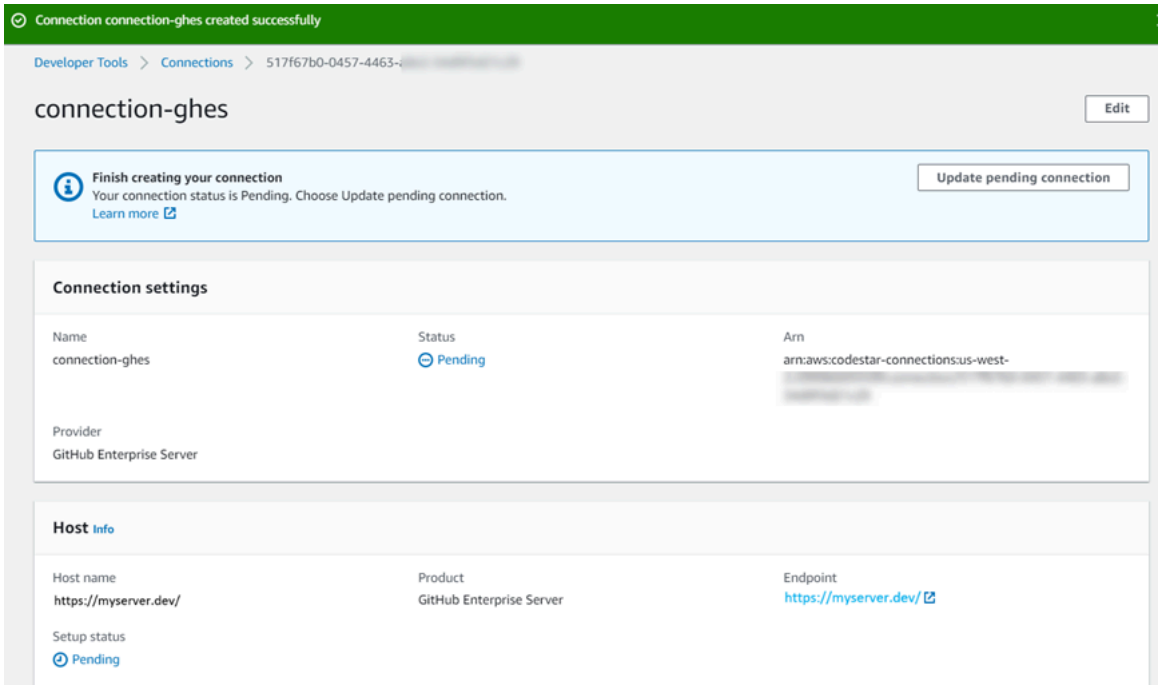
c. [Security group IDs] (セキュリティグループ ID) で、[Add] (追加) を選択します。このフィールドで、ホストに使用するセキュリティグループを選択します。最大 10 個のセキュリティグループを選択できます。

   GitHub Enterprise Server インスタンスがインストールされているインフラストラクチャのセキュリティグループ、または VPN または Direct Connect を介してインストールされた GitHub Enterprise Server インスタンスにアクセスできるセキュリティグループを選択してください。

d. プライベート VPC を設定していて、非公開認証局を使用して TLS 検証を実行するように GitHub Enterprise Server インスタンスを設定している場合は、[TLS証明書] に証明書 ID を入力します。TLS 証明書の値は、証明書のパブリックキーである必要があります。

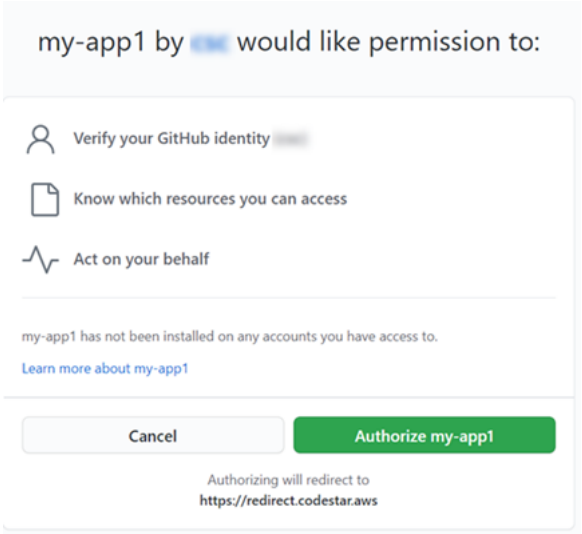


4. [Connect to GitHub Enterprise Server] (GitHub Enterprise Server に接続する) を選択します。作成された接続は、Pending (保留中) のステータスで表示されます。指定したサーバ情報との接続用に、ホストリソースが作成されます。ホスト名には、URL が使用されます。
5. 保留中の接続の更新を選択します。



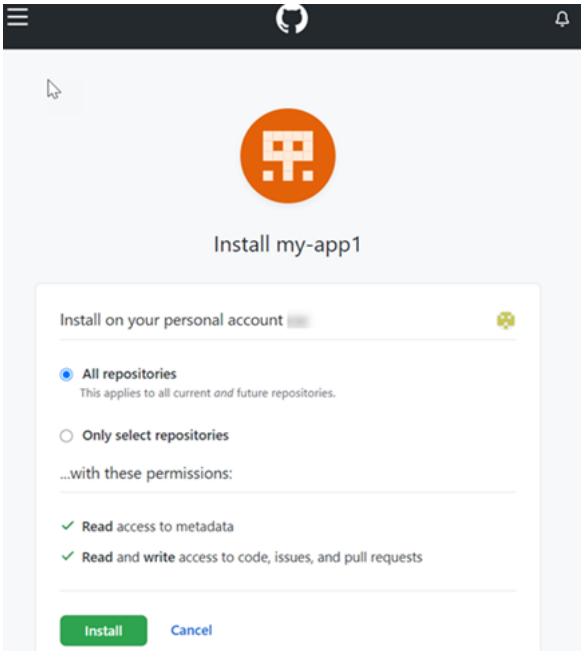
6. メッセージが表示されたら、GitHub Enterprise のログインページで、GitHub Enterprise の認証情報でサインインします。
7. [Create GitHub App] (GitHub アプリの作成) ページで、アプリの名前を選択します。

8. [GitHub の承認] ページで、[<app-name> を承認] を選択します。



9. [アプリインストール] ページに、コネクターアプリをインストールする準備ができたことを示すメッセージが表示されます。複数の組織がある場合は、アプリをインストールする組織を選択するように求められる場合があります。

   アプリをインストールするリポジトリ設定を選択します。[インストール] を選択します。



10. 接続ページには、作成された接続が Available (使用可能) ステータスで表示されます。

GitHub Enterprise Server への接続を作成する (CLI)

AWS Command Line Interface (AWS CLI) を使用して接続を作成できます。

これを行うには、create-host および create-connection コマンドを使用します。

> **Important**
>
> AWS CLI または を介して作成された接続 AWS CloudFormation は、デフォルトで PENDINGステータスです。CLI または との接続を作成したら CloudFormation、コンソールを使用して接続を編集し、ステータスを にしますAVAILABLE。

ステップ 1: GitHub Enterprise Server 用のホストを作成するには (CLI)

1. ターミナル (Linux/macOS/Unix) またはコマンドプロンプト (Windows) を開きます。 AWS CLI を使用して create-host コマンドを実行し、`--provider-endpoint`接続に `--name`、`--provider-type`、 を指定します。この例では、サードパーティープロバイダー名は `GitHubEnterpriseServer` で、エンドポイントは `my-instance.dev` です。

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

   成功した場合、このコマンドは次のようなホストの Amazonリソースネーム (ARN) 情報を返します。

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

   この手順の後、ホストのステータスは `PENDING` になります。

2. コンソールでホストのセットアップを完了し、ホストのステータスを `Available` に移行します。詳細については、「保留中のホストをセットアップする」を参照してください。

ステップ 2: コンソールで保留中のホストを設定するには

1. にサインイン AWS マネジメントコンソール し、 で開発者ツールコンソールを開きますhttps://console.aws.amazon.com/codesuite/settings/connections。
2. コンソールでホストのセットアップを完了し、ホストのステータスを `Available` に移行します。「保留中のホストをセットアップする」を参照してください。

ステップ 3: GitHub Enterprise Server 用の接続を作成するには (CLI)

1. ターミナル (Linux/macOS/Unix) またはコマンドプロンプト (Windows) を開きます。を使用して create-connection コマンド AWS CLI を実行し、接続`--connection-name`の `--host-arn`とを指定します。

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

   成功した場合、このコマンドは次のような接続 ARN 情報を返します。

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

2. コンソールを使用して、保留中の接続を設定します。詳細については、「保留中の接続の更新」を参照してください。

ステップ 4: コンソールで GitHub Enterprise Server への接続を完了するには

1. にサインイン AWS マネジメントコンソール し、 で開発者ツールコンソールを開きますhttps://console.aws.amazon.com/codesuite/settings/connections。
2. コンソールを使用して、保留中の接続を設定し、接続のステータスを `Available` に移行します。詳細については、「保留中の接続の更新」を参照してください。

GitLab への接続を作成する

AWS マネジメントコンソール または AWS Command Line Interface (AWS CLI) を使用して、gitlab.com でホストされているリポジトリへの接続を作成できます。

> **Note**
>
> この接続のインストールを GitLab で承認すると、データを処理するアクセス許可を当社のサービスに付与したものとみなされます。また、アプリケーションをアンインストールすれば、アクセス許可をいつでも取り消すことができます。

開始する前に:

- GitLab でアカウントを作成しておく必要があります。

> **Note**
>
> Connections は、接続の作成と承認に使用されたアカウント用のアクセスだけを提供します。

> **Note**
>
> GitLab で、自分が所有者ロールを持っている接続を作成すると、その接続を CodePipeline などのリソースを含むリポジトリで使用できます。グループ内のリポジトリでは、グループの所有者である必要はありません。

トピック

- GitLab (コンソール) への接続を作成する
- GitLab (CLI) への接続を作成する

GitLab (コンソール) への接続を作成する

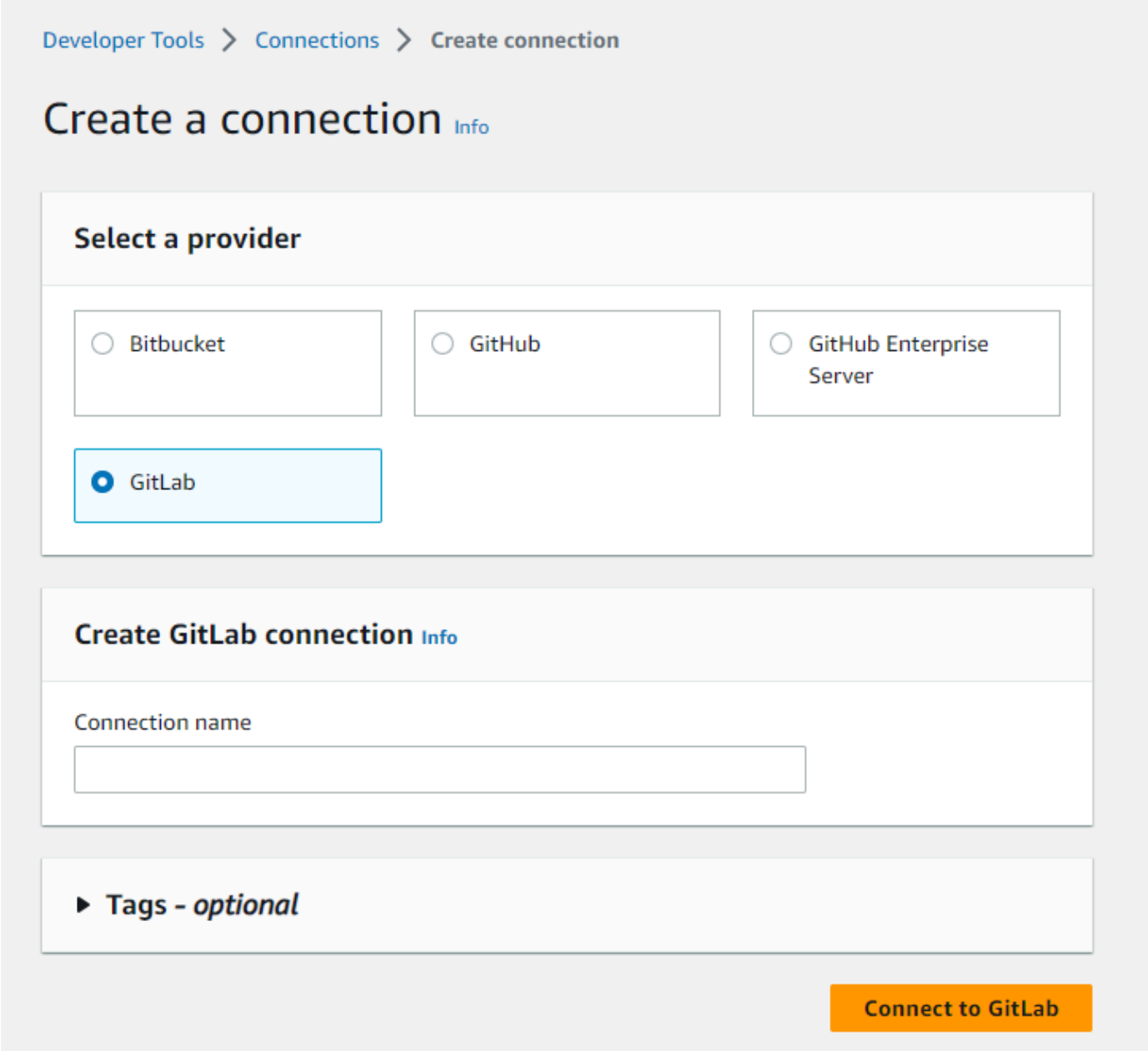
コンソールを使用して接続を作成できます。

> **Note**
>
> 2024 年 7 月 1 日以降、コンソールはリソース ARN `codeconnections`に との接続を作成します。両方のサービスプレフィックスを持つリソースは、コンソールに引き続き表示されます。

ステップ 1: 接続の作成

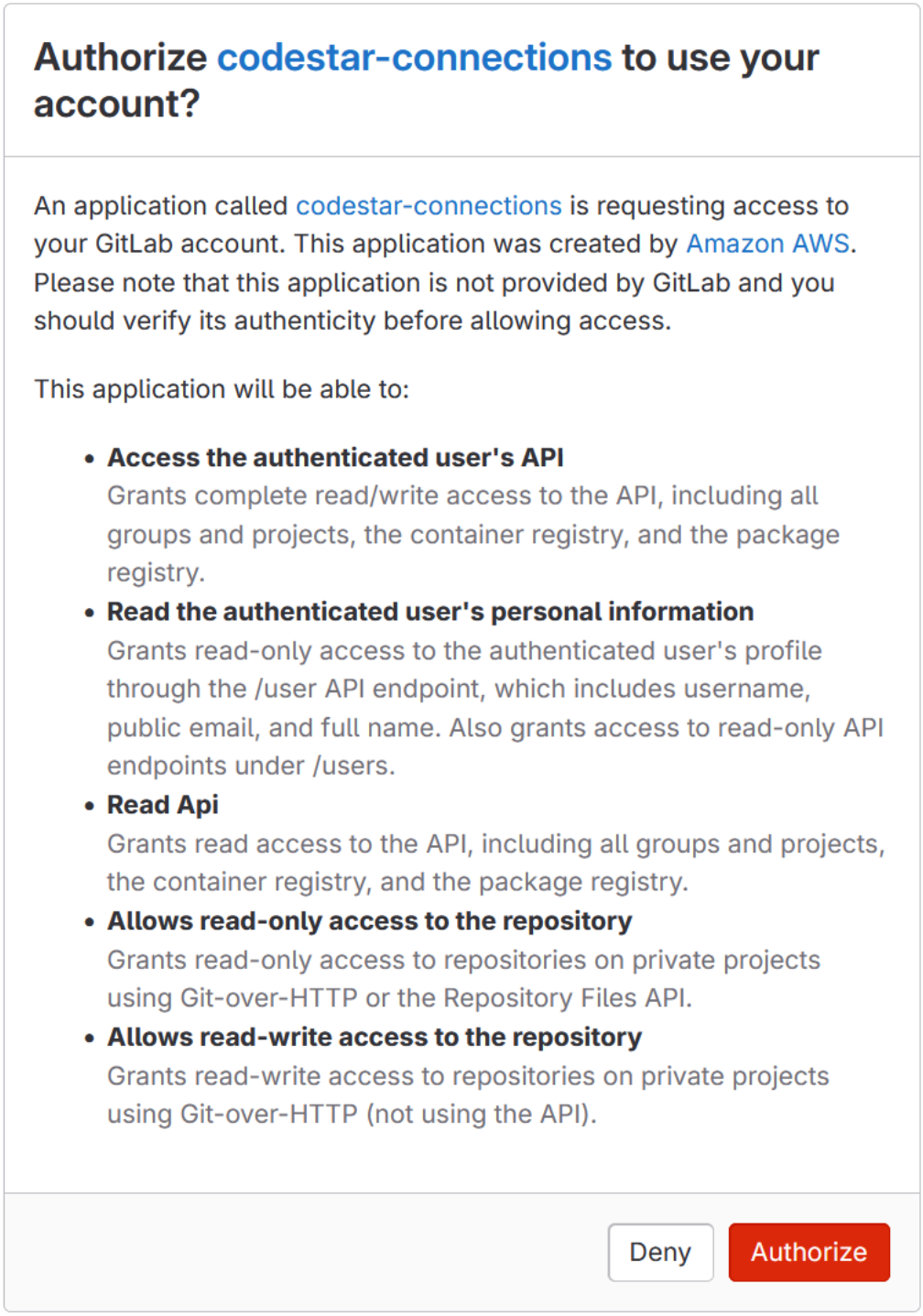
1. にサインインし AWS マネジメントコンソール、 で AWS 開発者ツールコンソールを開きますhttps://console.aws.amazon.com/codesuite/settings/connections。
2. [設定] を選択して、次に [接続] を選択します。[接続を作成] を選択します。

3. GitLab リポジトリへの接続を作成するには、[プロバイダーを選択する] で、[GitLab] を選択します。[接続名] に、作成する接続の名前を入力します。 [GitLab に接続] を選択します。



4. GitLab のサインインページが表示されたら、認証情報を使用してログインし、[サインイン] を選択します。
5. 認可ページが開き、GitLab アカウントにアクセスするための接続の認可を求めるメッセージが表示されます。

   [承認] を選択します。



6. ブラウザは接続コンソールページに戻ります。[GitLab 接続を作成] の下で、新しい接続は [接続名] に表示されます。
7. [GitLab に接続] を選択します。

接続が正常に作成されると、成功バナーが表示されます。接続の詳細は、[接続設定] ページに表示されます。

GitLab (CLI) への接続を作成する

AWS Command Line Interface (AWS CLI) を使用して接続を作成できます。

これを行うには、create-connection コマンドを使用します。

> **Important**
>
> AWS CLI または を介して作成された接続 AWS CloudFormation は、デフォルトで PENDINGステータスです。CLI または との接続を作成したら CloudFormation、コンソールを使用して接続を編集し、ステータスを にしますAVAILABLE。

GitLab への接続を作成するには

1. ターミナル (Linux/macOS/Unix) またはコマンドプロンプト (Windows) を開きます。 AWS CLI を使用して create-connection コマンドを実行し、接続--connection-nameの --provider-typeと を指定します。この例では、サードパーティープロバイダー名は GitLab で、指定された接続名は MyConnection です。

   ```
   aws codeconnections create-connection --provider-type GitLab --connection-name
    MyConnection
   ```

   成功した場合、このコマンドは次のような接続 ARN 情報を返します。

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

2. コンソールを使用して接続を完了します。詳細については、「保留中の接続の更新」を参照してください。

GitLab セルフマネージドへの接続を作成する

GitLab セルフマネージドのインストールで、Enterprise Edition または Community Edition 用の接続を作成できます。

AWS マネジメントコンソール または AWS Command Line Interface (AWS CLI) を使用して、GitLab セルフマネージド用の接続とホストを作成できます。

> **Note**
>
> この接続アプリケーションを GitLab セルフマネージドで承認すると、データを処理するアクセス許可を当社のサービスに付与したものとみなされます。また、アプリケーションをアンインストールすれば、アクセス許可をいつでも取り消すことができます。

GitLab セルフマネージドへの接続を作成する前に、以下のステップに示すように、接続に使用するホストを作成します。インストール済みプロバイダー用のホスト作成ワークフローの概要については、「ホストを作成または更新するワークフロー」を参照してください。

オプションで VPC を使用してホストを設定できます。ホストリソース用のネットワークおよび VPC 設定の詳細については、「(オプション) 前提条件: 接続用のネットワーク設定または Amazon VPC 設定」および「ホストの VPC 設定のトラブルシューティング」を参照してください。

開始する前に:

- GitLab でアカウントを作成済みで、セルフマネージドインストールの GitLab Enterprise Edition または GitLab Community Edition を持っている必要があります。詳細については、https://docs.gitlab.com/ee/subscriptions/self_managed/ を参照してください。

  > **Note**
  >
  > Connections は、接続の作成と承認に使用されたアカウント用のアクセスだけを提供します。

> **Note**
>
> GitLab で、自分が所有者ロールを持っているリポジトリへの接続を作成すると、その接続を CodePipeline などのリソースで使用できます。グループ内のリポジトリでは、グループの所有者である必要はありません。

- スコープダウンアクセス許可のみを持つ GitLab 個人用アクセストークン (PAT) を既に作成している必要があります: `api`、`admin_mode`。詳細については、https://docs.gitlab.com/ee/user/profile/personal_access_tokens.html を参照してください。PAT を作成して使用するには、管理者である必要があります。

> **Note**
>
> PAT はホストの認可に使用され、それ以外の方法で保存または接続に使用されることはありません。ホストを設定するには、一時的な PAT を作成し、ホストを設定した後に PAT を削除できます。

> **Note**
>
> GitHub Enterprise Server または GitLab セルフマネージドの組織では、使用可能なホストを渡しません。組織内の接続ごとに新しいホストを作成し、ホストのネットワークフィールド (VPC ID、サブネット IDs、セキュリティグループ IDs) に必ず同じ情報を入力する必要があります。詳細については、「組織をサポートするインストール済みプロバイダーの接続とホストのセットアップ」を参照してください。

トピック

- GitLab セルフマネージドへの接続を作成する (コンソール)
- GitLab セルフマネージドへの接続を作成する (CLI)

GitLab セルフマネージドへの接続を作成する (コンソール)

次のステップを使用してホストを作成し、コンソールで GitHub セルフマネージドへの接続を作成します。VPC でホストをセットアップする際の考慮事項については、「(オプション) 前提条件: 接続用のネットワーク設定または Amazon VPC 設定」を参照してください。

> **Note**
>
> 2024 年 7 月 1 日以降、コンソールはリソース ARN codeconnectionsに との接続を作成します。両方のサービスプレフィックスを持つリソースは、コンソールに引き続き表示されます。

> **Note**
>
> 単一の GitLab セルフマネージドインストール用のホストを作成し、そのホストへの 1 つ以上の GitLab セルフマネージド接続を管理できます。

ステップ 1: ホストを作成する

1. にサインインし AWS マネジメントコンソール、 で AWS 開発者ツールコンソールを開きますhttps://console.aws.amazon.com/codesuite/settings/connections。
2. [Hosts (ホスト)]タブで、[Create host (ホストの作成)]を選択します。
3. [ホスト名]に、ホストに使用する名前を入力します。
4. [プロバイダーを選択] で、[GitLab セルフマネージド] を選択します。
5. [URL] に、プロバイダーがインストールされているインフラストラクチャのエンドポイントを入力します。
6. サーバーが Amazon VPC 内に設定されていて、VPC に接続する場合は、 Use a VPC (VPC を使用) を選択します。それ以外の場合、[No VPC] を選択します。
7. (オプション) Amazon VPC でホストを起動し、VPC に接続する場合は、[VPC を使用] を選択して、以下を完了します。

   > **Note**
   >
   > GitHub Enterprise Server または GitLab セルフマネージドの組織では、使用可能なホストを渡しません。組織内の接続ごとに新しいホストを作成し、ホストのネットワーク

フィールド (VPC ID、サブネット IDs、セキュリティグループ IDs) に必ず同じ情報を入力する必要があります。詳細については、「組織をサポートするインストール済みプロバイダーの接続とホストのセットアップ」を参照してください。

a. [VPC ID] で、 VPC ID を選択します。ホストがインストールされているインフラストラクチャに VPC を選択するか、VPN または Direct Connect を介してインスタンスにアクセスできる VPC を選択します。

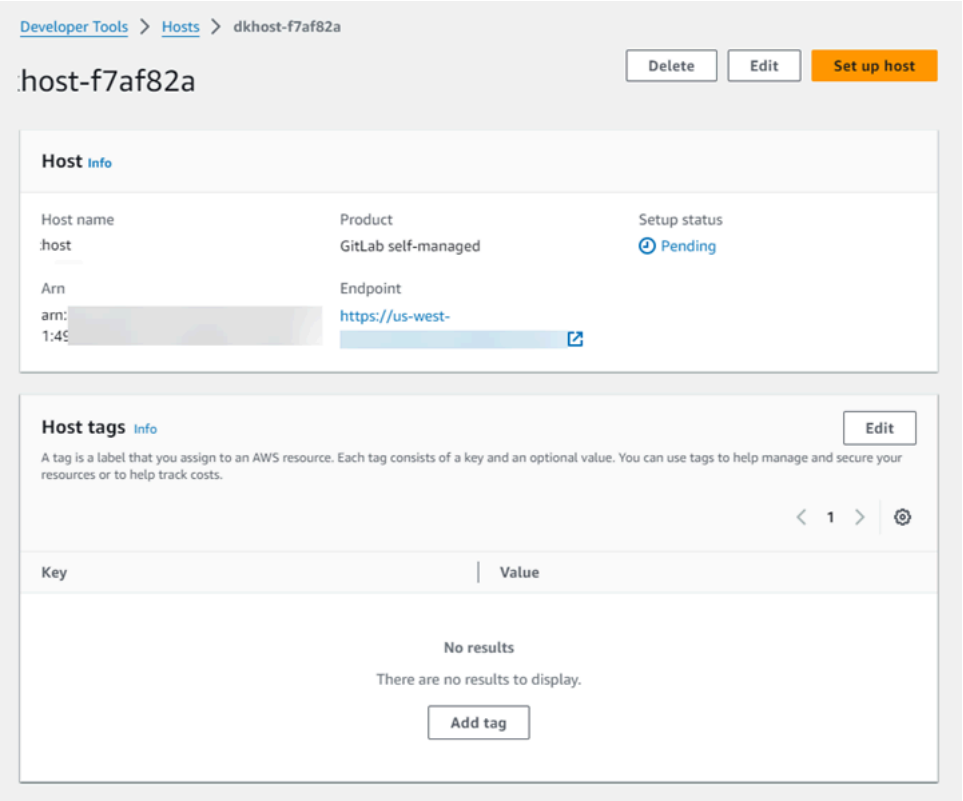
b. プライベート VPC を設定していて、非公開認証局を使用して TLS 検証を実行するようにホストを設定している場合は、[TLS 証明書] に証明書 ID を入力します。TLS 証明書の値 は証明書のパブリックキーです。

8. [Create host] (ホストの作成) を選択します。

9. ホストの詳細ページが表示されたら、ホストの作成に伴ってホストのステータスが変化します。

> **Note**
>
> ホスト設定に VPC 設定が含まれている場合は、ホストネットワークコンポーネントのプロビジョニングに数分間かかります。

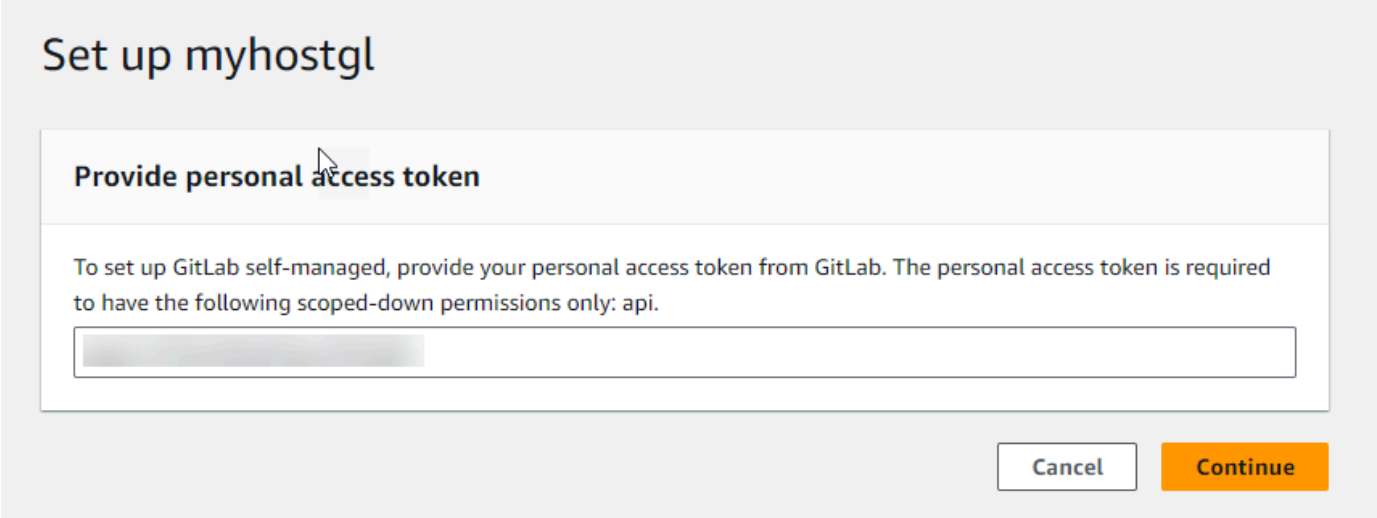
ホストのステータスがPending (保留中) になるのを待ってから、セットアップを完了します。詳細については、「保留中のホストをセットアップする」を参照してください。



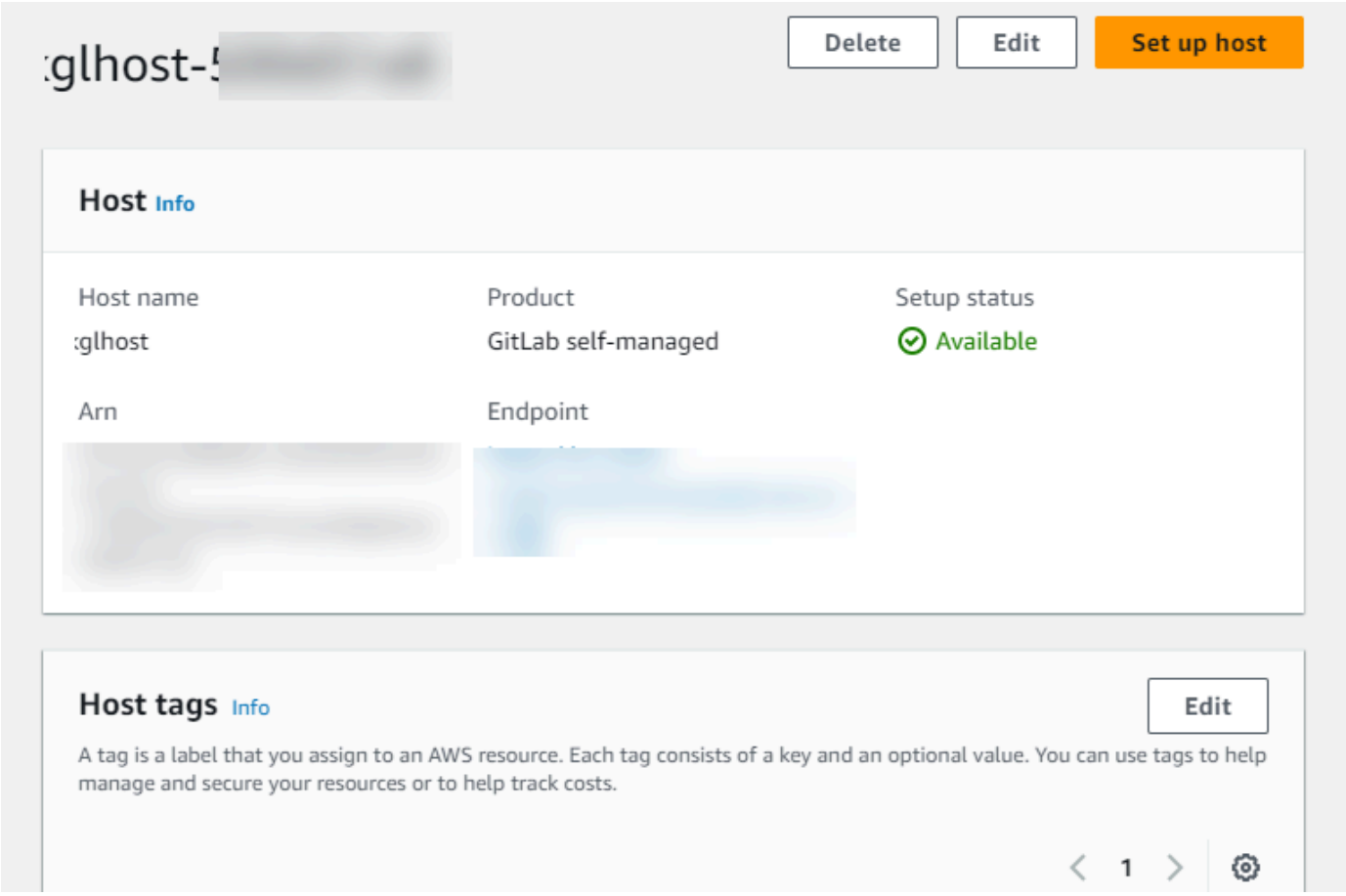
ステップ 2: 保留中のホストを設定する

1. [ホストをセットアップ] を選択します。
2. [***host_name*** のセットアップ] ページが表示されます。「個人用アクセストークンを提供する」で、GitLab PAT にスコープダウンされたアクセス許可のみを提供します。 `api`および `admin_mode`。

> **Note**
>
> PAT を作成して使用できるのは管理者のみです。

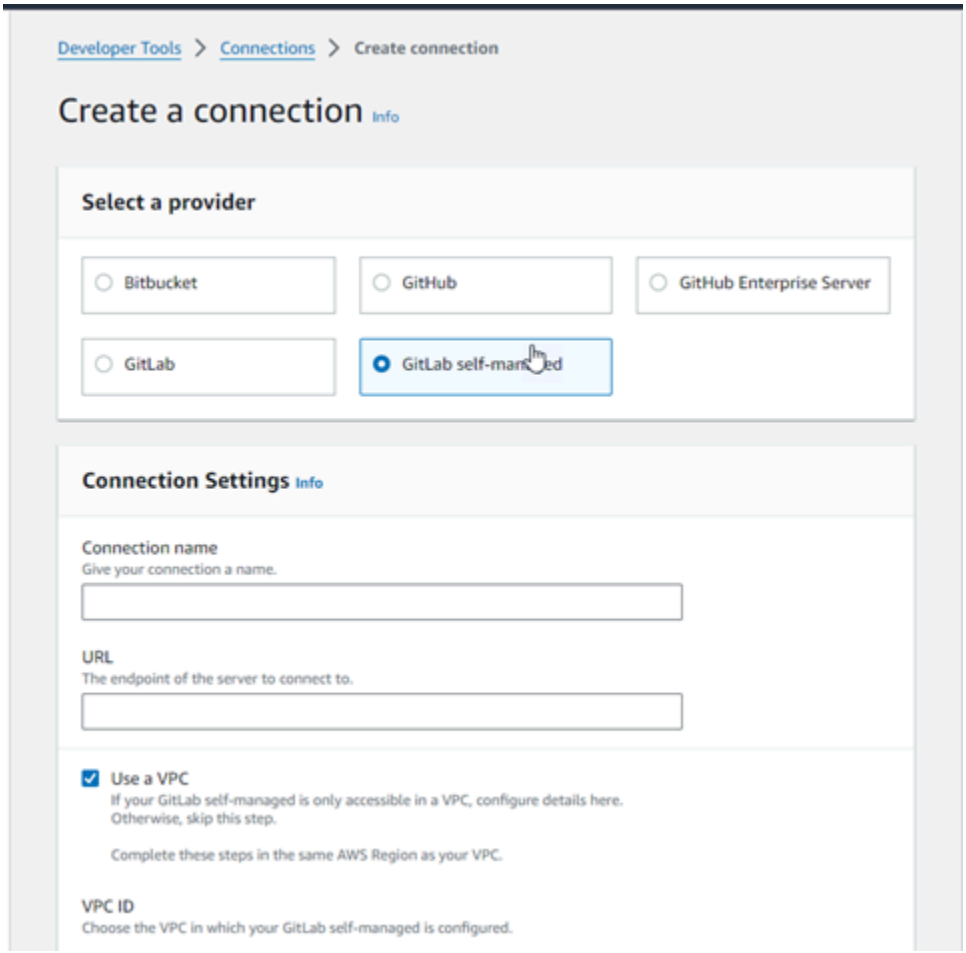


3. ホストが正常に登録されると、ホストの詳細ページが表示され、ホストのステータスが Available (使用可能) になります。



ステップ 3: 接続を作成する

1. にサインインし AWS マネジメントコンソール、 で AWS 開発者ツールコンソールを開きますhttps://console.aws.amazon.com/codesuite/settings/connections。
2. [設定] を選択して、次に [接続] を選択します。[接続を作成] を選択します。
3. GitLab リポジトリへの接続を作成するには、[プロバイダーを選択する] で、[GitLab セルフマネージド] を選択します。[接続名] に、作成する接続の名前を入力します。



4. [URL] に、サーバーのエンドポイントを入力します。
5. Amazon VPC でサーバーを起動し、VPC に接続する場合は、[Use a VPC] (VPC を使用) をクリックして、以下を完了します。

   a. [VPC ID] で、 VPC ID を選択します。ホストがインストールされているインフラストラクチャに VPC を選択するか、VPN または Direct Connect を介してホストにアクセスできる VPC を選択します。

   b. [サブネット ID] で、[Add] を選択します。このフィールドで、ホストに使用するサブネット ID を選択します。最大 10 個のサブネットを選択できます。

ホストがインストールされているインフラストラクチャにサブネットを選択するか、VPN または Direct Connect を介してインストールされたホストにアクセスできるサブネットを選択します。

c. [Security group IDs] (セキュリティグループ ID) で、[Add] (追加) を選択します。このフィールドで、ホストに使用するセキュリティグループを選択します。最大 10 個のセキュリティグループを選択できます。

ホストがインストールされているインフラストラクチャにセキュリティグループを選択するか、VPN または Direct Connect を介してインストールされたホストにアクセスできるセキュリティグループを選択します。

d. プライベート VPC を設定していて、非公開認証局を使用して TLS 検証を実行するようにホストを設定している場合は、[TLS 証明書] に証明書 ID を入力します。TLS 証明書の値は、証明書のパブリックキーである必要があります。

6. [GitLab セルフマネージドへの接続] を選択します。作成された接続は、Pending (保留中) のステータスで表示されます。指定したサーバ情報との接続用に、ホストリソースが作成されます。ホスト名には、URL が使用されます。
7. 保留中の接続の更新を選択します。
8. GitLab のサインインページが表示されたら、認証情報を使用してログインし、[サインイン] を選択します。
9. 認可ページが開き、GitLab アカウントにアクセスするための接続の認可を求めるメッセージが表示されます。

[承認] を選択します。

10. ブラウザは接続コンソールページに戻ります。[GitLab 接続を作成] の下で、新しい接続は [接続名] に表示されます。
11. [GitLab セルフマネージドへの接続] を選択します。

接続が正常に作成されると、成功バナーが表示されます。接続の詳細は、[接続設定] ページに表示されます。

GitLab セルフマネージドへの接続を作成する (CLI)

AWS Command Line Interface (AWS CLI) を使用して、GitLab セルフマネージドのホストと接続を作成できます。

これを行うには、create-host および create-connection コマンドを使用します。

> **Important**
>
> AWS CLI または を介して作成された接続 AWS CloudFormation は、デフォルトで PENDINGステータスです。CLI または との接続を作成したら CloudFormation、コンソールを使用して接続を編集し、ステータスを にしますAVAILABLE。

ステップ 1: GitLab セルフマネージドのホストを作成するには (CLI)

1. ターミナル (Linux/macOS/Unix) またはコマンドプロンプト (Windows) を開きます。 AWS CLI を使用して create-host コマンドを実行し、--provider-endpoint接続に --name、--provider-type、 を指定します。この例では、サードパーティープロバイダー名は GitLabSelfManaged で、エンドポイントは my-instance.dev です。

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

   成功した場合、このコマンドは次のようなホストの Amazonリソースネーム (ARN) 情報を返します。

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

   この手順の後、ホストのステータスは PENDING になります。

2. コンソールを使用してホストのセットアップを完了し、次のステップでホストのステータスを Available に移行します。

ステップ 2: コンソールで保留中のホストを設定するには

1. にサインイン AWS マネジメントコンソール し、 で開発者ツールコンソールを開きますhttps://console.aws.amazon.com/codesuite/settings/connections。
2. コンソールでホストのセットアップを完了し、ホストのステータスを Available に移行します。「保留中のホストをセットアップする」を参照してください。

ステップ 3: GitLab セルフマネージドの接続を作成する (CLI)

1. ターミナル (Linux/macOS/Unix) またはコマンドプロンプト (Windows) を開きます。を使用して create-connection コマンド AWS CLI を実行し、接続--connection-nameの --host-arnとを指定します。

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

成功した場合、このコマンドは次のような接続 ARN 情報を返します。

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

2. 次のステップでコンソールを使用して、保留中の接続を設定します。

ステップ 4: コンソールで GitHub セルフマネージド用の接続を完了するには

1. にサインイン AWS マネジメントコンソール し、 で開発者ツールコンソールを開きますhttps://console.aws.amazon.com/codesuite/settings/connections。
2. コンソールを使用して、保留中の接続を設定し、接続のステータスを Available に移行します。詳細については、「保留中の接続の更新」を参照してください。

保留中の接続の更新

AWS Command Line Interface (AWS CLI) または を介して作成された接続 AWS CloudFormation は、デフォルトで PENDINGステータスです。 AWS CLI または との接続を作成したら CloudFormation、コンソールを使用して接続を更新し、ステータスを にしますAVAILABLE。

> **Note**
>
> 保留中の接続を更新するには、コンソールを使用する必要があります。 AWS CLIを使用して保留中の接続を更新できません。

コンソールを初めて使用してサードパーティープロバイダーに新しい接続を追加するときは、接続に関連付けられたインストールを使用して、サードパーティープロバイダと OAuth ハンドシェイクを完了する必要があります。

デベロッパーツールコンソールを使用して、保留中の接続を完了できます。

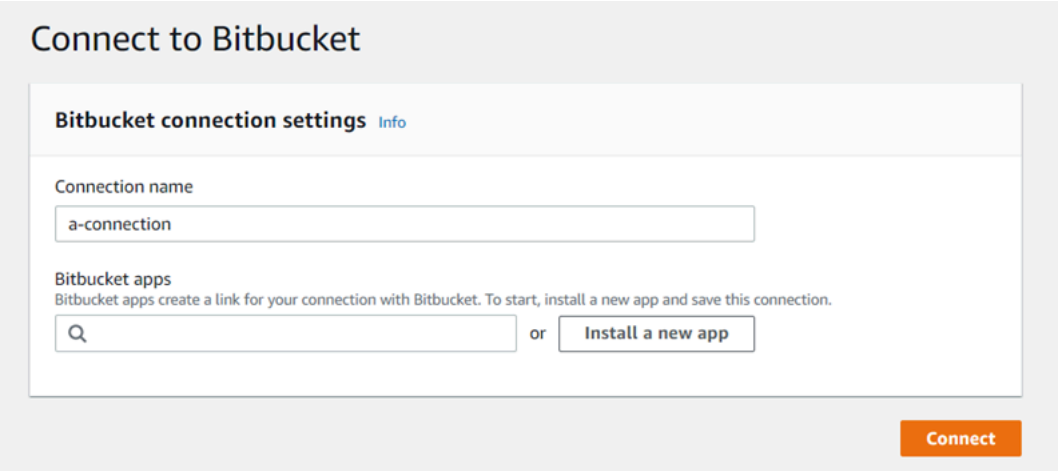
接続を完了するには

1. で AWS デベロッパーツールコンソールを開きますhttps://console.aws.amazon.com/codesuite/settings/connections。
2. [設定] > [接続] を選択します。

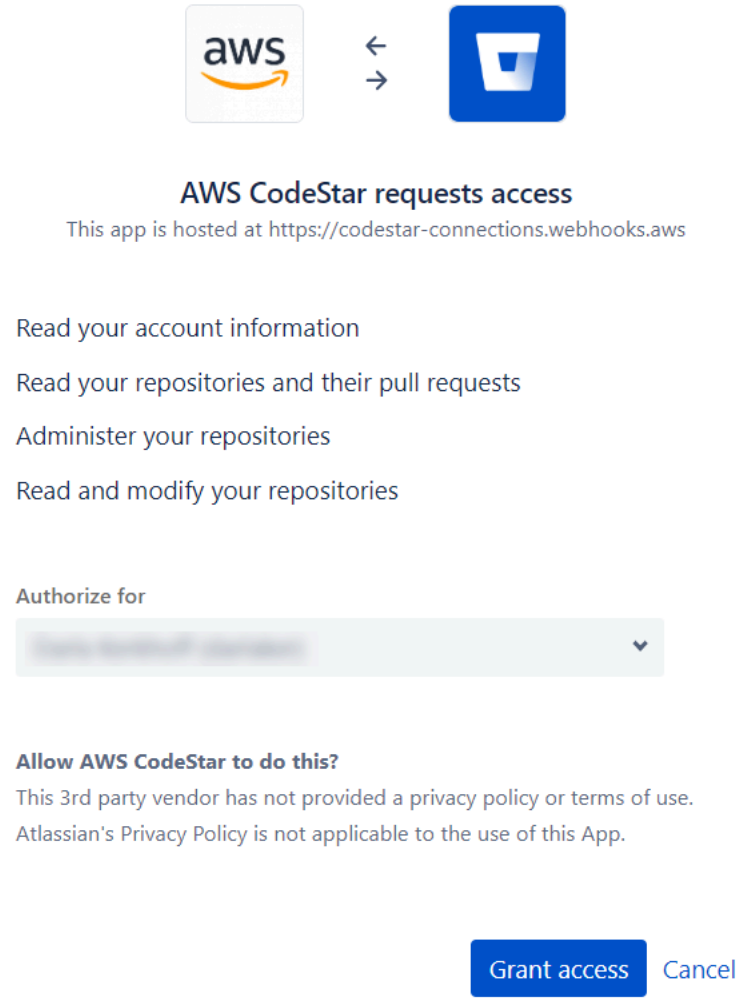
   AWS アカウントに関連付けられているすべての接続の名前が表示されます。
3. [Name (名前)] で、更新する保留中の接続の名前を選択します。

   Pending (保留中) ステータスの接続を選択すると、Update connection (接続の更新) が有効になります。
4. [保留中の接続の更新]を選択します。
5. [Connect to Bitbucket] (Bitbucket に接続) ページの [Connection name] (接続名) で、接続名を確認します。

   [Bitbucket apps] (Bitbucket アプリ) で、アプリのインストールを選択するか、[Install a new app] (新しいアプリをインストールする) を選択してアプリを作成します。



6. アプリのインストールページで、 AWS CodeStar アプリが Bitbucket アカウントに接続しようとしていることを示すメッセージが表示されます。[アクセス権の付与] を選択します。



7. 新規インストールの接続 ID が表示されます。[Complete connection (接続の完了)] を選択します。

接続を一覧表示する

開発者用ツールコンソールまたは AWS Command Line Interface (AWS CLI) 内の list-connections コマンドを使用して、アカウント内の接続のリストを表示できます。

接続を一覧表示する (コンソール)

接続を一覧表示するには

1. https://console.aws.amazon.com/codesuite/settings/connections でデベロッパーツールコンソールを開きます。
2. [設定] > [接続] を選択します。

3. 接続の名前、ステータス、および ARN を表示します。

接続を一覧表示する (CLI)

を使用して AWS CLI 、サードパーティーのコードリポジトリへの接続を一覧表示できます。GitHub Enteprise Server への接続など、ホストリソースに関連付けられた接続の場合、出力はホスト ARN も返します。

これを行うには、list-connections コマンドを使用します。

接続を一覧表示するには

- ターミナル (Linux、macOS、または Unix) またはコマンドプロンプト (Windows) を開き、AWS CLI を使用してlist-connectionsコマンドを実行します。

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

このコマンドで、以下の出力が返ります。

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

接続を削除

デベロッパーツールコンソールまたは AWS Command Line Interface (AWS CLI) の delete-connection コマンドを使用して、接続を削除できます。

トピック

接続を削除する (コンソール)

接続を削除する方法

1. https://console.aws.amazon.com/codesuite/settings/connections でデベロッパーツールコンソールを開きます。
2. [設定] > [接続] を選択します。
3. [Connection name (接続名)] で、削除する接続の名前を選択します。
4. [削除] を選択します。
5. フィールドに「**delete**」と入力して確認し、[Delete (削除)] を選択します。

> **Important**
>
> このアクションを元に戻すことはできません。

接続を削除する (CLI)

AWS Command Line Interface (AWS CLI) を使用して接続を削除できます。

これを行うには、delete-connection コマンドを使用します。

> **Important**
>
> コマンドを実行すると、接続は削除されます。確認のダイアログボックスは表示されません。新しい接続を作成することはできますが、Amazon リソースネーム (ARN) は再利用されません。

接続を削除する方法

- ターミナル (Linux/macOS/Unix) またはコマンドプロンプト (Windows) を開きます。 AWS CLI を使用して delete-connection コマンドを実行し、削除する接続の ARN を指定します。

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

  このコマンドは何も返しません。

タグ接続リソース

タグは、 AWS リソース AWS に割り当てるカスタム属性ラベルです。各 AWS タグには 2 つの部分があります。

- タグキー (例： CostCenter、Environment、または Project)。タグキーでは大文字と小文字が区別されます。
- タグ値と呼ばれるオプションのフィールド (111122223333、Production、チーム名など)。タグ値を省略すると、空の文字列を使用した場合と同じになります。タグキーと同様に、タグ値では大文字と小文字が区別されます。

これらは共にキーと値のペアと呼ばれます。

コンソールまたは CLI を使用して、リソースのタグ付けをします。

AWS CodeConnections では、次のリソースタイプにタグを付けることができます。

- Connections
- [ホスト]

これらのステップでは、 の最新バージョンが既にインストールされているか、最新バージョンに AWS CLI 更新されていることを前提としています。詳細については、「AWS Command Line Interface ユーザーガイド」の「Installing the AWS CLI」を参照してください。

タグを使用してリソースを識別、整理、追跡するだけでなく、 AWS Identity and Access Management (IAM) ポリシーのタグを使用して、リソースを表示および操作できるユーザーを制御できます。タグベースのアクセスポリシーの例については、「タグを使用して AWS CodeConnections リソースへのアクセスを制御する」を参照してください。

トピック

- リソースのタグ付け (コンソール)
- タグリソース (CLI)

リソースのタグ付け (コンソール)

コンソールを使用して、接続リソースにタグを追加、更新、または削除できます。

トピック

- 接続リソースにタグを追加する (コンソール)
- 接続リソース (コンソール) のタグを表示する
- 接続リソース (コンソール) のタグを編集する
- 接続リソースからのタグを削除する (コンソール)

接続リソースにタグを追加する (コンソール)

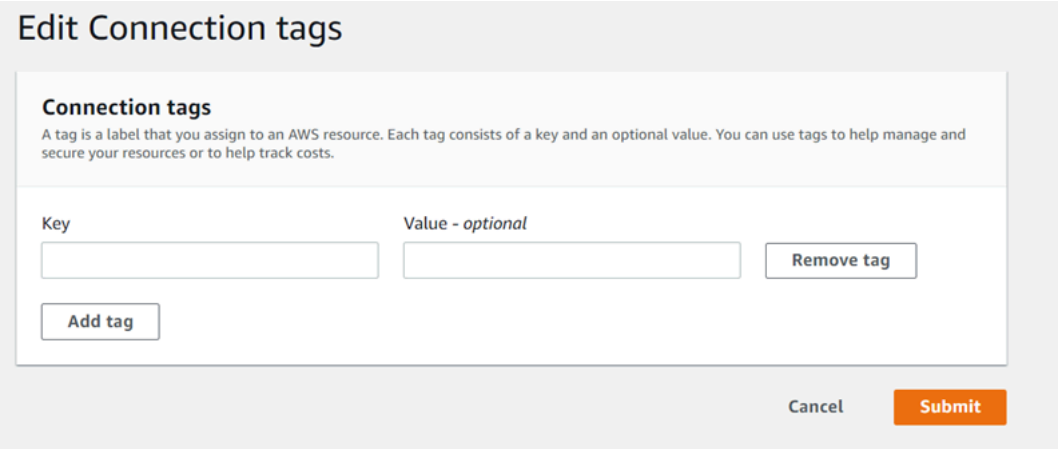
コンソールを使用して、既存の接続またはホストにタグを追加します。

> **Note**
>
> GitHub Enterprise Server などのインストール済みプロバイダーの接続を作成し、ホストリソースも作成すると、作成中のタグはこの接続だけに追加されます。これにより、ホストを新しい接続で再利用する場合は、ホストに個別にタグを付けることができます。ホストにタグを追加するには、次の手順に従います。

接続にタグを追加するには

1. コンソールにサインインします。ナビゲーションパネルから [Settings (設定)] を選択します。
2. [Settings] (設定) で、[Connections] (接続) を選択します。[Connections (接続)] タブを選択します。
3. 編集する接続を選択します。接続設定のページが表示されます。
4. [Connection tags] (接続タグ) で、[Edit] (編集) を選択します。[Edit Connection tags] (接続タグの編集) ページが表示されます。

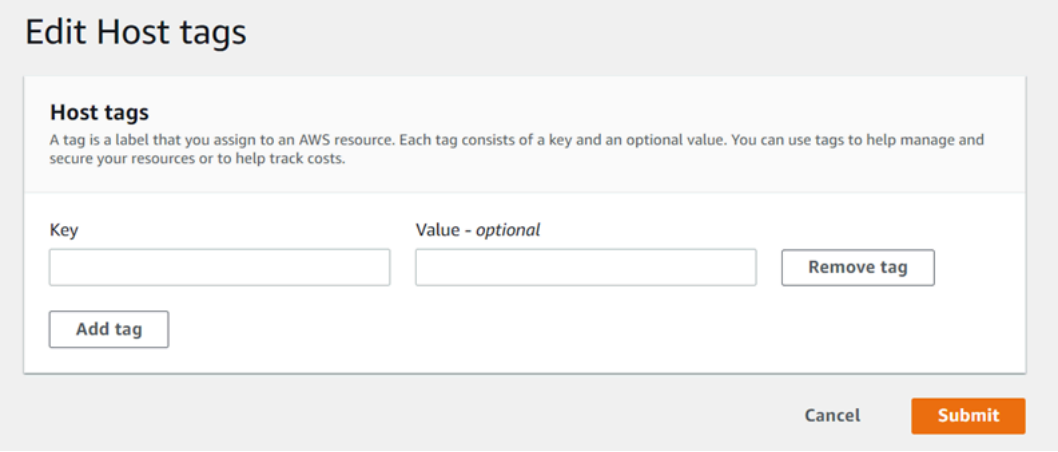
5. [Key] フィールドと [Value] フィールドに、追加するタグのセットごとにキーペアを入力します。([値] フィールドはオプションです。) 例えば、[キー] では、「**Project**」と入力します。[値] には「**ProjectA**」と入力します。



6. (オプション) [タグを追加] をクリックして行を追加し、さらにタグを入力します。
7. [Submit] を選択してください。タグは、接続の設定の下に表示されます。

ホストにタグを追加するには

1. コンソールにサインインします。ナビゲーションパネルから [Settings (設定)] を選択します。
2. [Settings] (設定) で、[Connections] (接続) を選択します。[Hosts] (ホスト) タブを選択します。
3. 編集するホストを選択します。ホスト設定のページが表示されます。
4. [Host tags] (ホストタグ) で、[Edit] (編集) を選択します。[Hosts Tag] (ホストタグ) ページが表示されます。
5. [Key] フィールドと [Value] フィールドに、追加するタグのセットごとにキーペアを入力します。([値] フィールドはオプションです。) 例えば、[キー] では、「**Project**」と入力します。[値] には「**ProjectA**」と入力します。



6. (オプション) [Add tag] (タグの追加) を選択して行を追加し、さらにホストのタグを入力します。
7. [Submit] を選択してください。タグは、ホストの設定の下に表示されます。

接続リソース (コンソール) のタグを表示する

コンソールを使用して、既存のリソースのタグを表示できます。

接続のタグを表示するには

1. コンソールにサインインします。ナビゲーションパネルから [Settings (設定)] を選択します。
2. [Settings] (設定) で、[Connections] (接続) を選択します。[Connections (接続)] タブを選択します。
3. 表示する接続を選択します。接続設定のページが表示されます。
4. [Connection tags] で、[Key] 列と [Value] 列下の接続のタグを表示します。

ホストのタグを表示するには

1. コンソールにサインインします。ナビゲーションパネルから [Settings (設定)] を選択します。
2. [Settings] (設定) で、[Connections] (接続) を選択します。[Hosts] (ホスト) タブを選択します。
3. 表示するホストを選択します。
4. [Host tags] で、[Key] 列と [Value] 列下のホストのタグを表示します。

接続リソース (コンソール) のタグを編集する

コンソールを使用して、接続リソースに追加されたタグを編集します。

接続のタグを編集するには

1. コンソールにサインインします。ナビゲーションパネルから [Settings (設定)] を選択します。
2. [Settings] (設定) で、[Connections] (接続) を選択します。[Connections (接続)] タブを選択します。
3. 編集する接続を選択します。接続設定のページが表示されます。
4. [Connection tags] (接続タグ) で、[Edit] (編集) を選択します。[Connection tags] (接続タグ) ページが表示されます。

5. [キー] フィールドと [値] フィールドに、必要に応じて各フィールドの値を更新します。例えば、**Project** キーの場合は、[Value] で、**ProjectA** を **ProjectB** に変更します。
6. [Submit] を選択してください。

ホストのタグを編集するには

1. コンソールにサインインします。ナビゲーションパネルから [Settings (設定)] を選択します。
2. [Settings] (設定) で、[Connections] (接続) を選択します。[Hosts] (ホスト) タブを選択します。
3. 編集するホストを選択します。ホスト設定のページが表示されます。
4. [Host tags] (ホストタグ) で、[Edit] (編集) を選択します。[Hosts Tag] (ホストタグ) ページが表示されます。
5. [キー] フィールドと [値] フィールドに、必要に応じて各フィールドの値を更新します。例えば、**Project** キーの場合は、[Value] で、**ProjectA** を **ProjectB** に変更します。
6. [Submit] を選択してください。

接続リソースからのタグを削除する (コンソール)

コンソールを使用して、接続リソースからタグを削除できます。関連付けられているリソースからタグを削除すると、そのタグが削除されます。

接続のタグを削除するには

1. コンソールにサインインします。ナビゲーションパネルから [Settings (設定)] を選択します。
2. [Settings] (設定) で、[Connections] (接続) を選択します。[Connections (接続)] タブを選択します。
3. 編集する接続を選択します。接続設定のページが表示されます。
4. [Connection tags] (接続タグ) で、[Edit] (編集) を選択します。[Connection tags] (接続タグ) ページが表示されます。
5. 削除する各タグのキーと値の横にある [Remove tag] を選択します。
6. [Submit] を選択してください。

ホストのタグを削除するには

1. コンソールにサインインします。ナビゲーションパネルから [Settings (設定)] を選択します。
2. [Settings] (設定) で、[Connections] (接続) を選択します。[Hosts] (ホスト) タブを選択します。

3. 編集するホストを選択します。ホスト設定のページが表示されます。
4. [Host tags] (ホストタグ) で、[Edit] (編集) を選択します。[Hosts Tag] (ホストタグ) ページが表示されます。
5. 削除する各タグのキーと値の横にある [Remove tag] を選択します。
6. [Submit] を選択してください。

タグリソース (CLI)

CLI を使用して、接続リソースのタグを表示、追加、更新、または削除できます。

トピック

- 接続リソースにタグを追加する (CLI)
- 接続リソース (CLI) のタグを表示する
- 接続リソース (CLI) のタグを編集する
- 接続リソース (CLI) からのタグを削除する

接続リソースにタグを追加する (CLI)

を使用して AWS CLI 、接続内のリソースにタグを付けることができます。

ターミナルまたはコマンドラインで、タグを追加するリソースの Amazon リソースネーム (ARN)、および追加するタグのキーと値を指定して tag-resource コマンドを実行します。複数のタグを追加できます。

接続にタグを追加するには

1. リソースの ARN を取得します。接続を一覧表示する に示されている list-connections コマンドを使用して、接続ARNを取得します。
2. ターミナルまたはコマンドラインで、tag-resource コマンドを実行します。

   例えば、次のコマンドを使用して、接続に 2 つのタグ、*Project* という名前のタグキーに *ProjectA* のタグ値、および *ReadOnly* という名前のタグキーに *true* のタグ値を付けます。

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

成功した場合、このコマンドは何も返しません。

ホストにタグを追加するには

1. リソースの ARN を取得します。ホストを一覧表示 に示されている list-hosts コマンドを使用して、ホスト ARN を取得します。
2. ターミナルまたはコマンドラインで、tag-resource コマンドを実行します。

   例えば、次のコマンドを使用して、ホストに 2 つのタグ、*Project* という名前のタグキーに *ProjectA* のタグ値、および *IscontainerBased* という名前のタグキーに *true* のタグ値を付けます。

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

   成功した場合、このコマンドは何も返しません。

接続リソース (CLI) のタグを表示する

を使用して AWS CLI 、接続リソースの AWS タグを表示できます。タグが追加されていない場合、返されるリストは空になります。を使用する list-tags-for-resource コマンドを使用して、接続またはホストに追加されたタグを表示します。

接続のタグを表示するには

1. リソースの ARN を取得します。接続を一覧表示する に示されている list-connections コマンドを使用して、接続ARNを取得します。
2. ターミナルまたはコマンドラインで、list-tags-for-resource コマンドを実行します。例えば、接続のタグキーとタグ値の一覧を表示するには、次のコマンドを使用します。

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

   このコマンドは、リソースに関連付けられているタグを返します。この例は、接続に対して返される 2 つのキーと値のペアを示しています。

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

ホストのタグを表示するには

1. リソースの ARN を取得します。ホストを一覧表示 に示されている list-hosts コマンドを使用して、ホスト ARN を取得します。
2. ターミナルまたはコマンドラインで、list-tags-for-resource コマンドを実行します。例えば、 ホストのタグキーとタグ値の一覧を表示するには、次のコマンドを使用します。

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

このコマンドは、リソースに関連付けられているタグを返します。この例は、ホストに対して返される 2 つのキーと値のペアを示しています。

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

接続リソース (CLI) のタグを編集する

を使用して AWS CLI 、リソースのタグを編集できます。既存のキーの値を変更したり、別のキーを追加できます。

ターミナルまたはコマンドラインで、タグを更新するリソースの ARN を指定して、tag-resource コマンドを実行し、更新するタグキーとタグ値を指定します。

タグを編集すると、指定されていないタグキーは保持されますが、同じキーで新しい値を持つものはすべて更新されます。edit コマンドで追加された新しいキーは、新しいキーと値のペアとして追加されます。

接続のタグを編集するには

1. リソースの ARN を取得します。接続を一覧表示する に示されている list-connections コマンドを使用して、接続ARNを取得します。
2. ターミナルまたはコマンドラインで、tag-resource コマンドを実行します。

   この例では、キーの値 `Project` が `ProjectB` に変更されています。

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

   成功した場合、このコマンドは何も返しません。接続に関連付けられているタグを確認するには、list-tags-for-resource コマンドを実行します。

ホストのタグを編集するには

1. リソースの ARN を取得します。ホストを一覧表示 に示されている list-hosts コマンドを使用して、ホスト ARN を取得します。
2. ターミナルまたはコマンドラインで、tag-resource コマンドを実行します。

   この例では、キーの値 `Project` が `ProjectB` に変更されています。

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

成功した場合、このコマンドは何も返しません。ホストに関連付けられているタグを確認するには、list-tags-for-resource コマンドを実行します。

接続リソース (CLI) からのタグを削除する

を使用してリソースからタグ AWS CLI を削除するには、次の手順に従います。関連付けられているリソースからタグを削除すると、そのタグが削除されます。

> **Note**
>
> 接続リソースを削除すると、削除されたリソースからすべてのタグの関連付けが削除されます。接続リソースを削除する前に、タグを削除する必要はありません。

ターミナルまたはコマンドラインで、タグを削除するリソースの ARN と削除するタグのタグキーを指定して、untag-resource コマンドを実行します。例えば、タグキー *Project* および *ReadOnly* を持つ接続の複数のタグを削除するには、次のコマンドを使用します。

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

成功した場合、このコマンドは何も返しません。リソースに関連付けられているタグを確認するには、list-tags-for-resource コマンドを実行します。出力は、すべてのタグが削除されたことを示しています。

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

接続の詳細の表示

デベロッパーツールコンソールまたは AWS Command Line Interface (AWS CLI) の get-connection コマンドを使用して、接続の詳細を表示できます。を使用するには AWS CLI、 の最新バージョンがインストールされている AWS CLI か、最新バージョンに更新されている必要があります。詳細については、「AWS Command Line Interface ユーザーガイド」の「Installing the AWS CLI」を参照してください。

接続を表示するには (コンソール)

1. https://console.aws.amazon.com/codesuite/settings/connections でデベロッパーツールコンソールを開きます。
2. [設定] > [接続] を選択します。
3. 表示する接続の横にあるボタンを選択して、[View details] をクリックします。
4. 接続に関する次の情報が表示されます。
   - 接続名。
   - 接続のプロバイダータイプ。
   - 接続ステータス。
   - 接続 ARN。
   - GitHub Enterprise Server などのインストール済みプロバイダー向けに接続が作成された場合、ホスト情報は接続に関連付けられます。
   - GitHub Enterprise Server などインストール済みプロバイダー向けに接続が作成された場合、エンドポイント情報は接続のホストに関連付けられます。
5. 接続のステータスが Pending (保留中) のときに接続を完了するには、保留中の接続の更新を選択します。詳細については、「Update a pending connection」を参照してください。

接続を表示するには (CLI)

- ターミナルまたはコマンドラインで、get-connection コマンドを実行します。例えば、`arn:aws:codestar-connections:us-west-2:account_id:connection/aEXAMPLE-8aad-4d5d-8878-dfcab0bc441f` ARN 値を持つ接続の詳細を表示するには、次のコマンドを使用します。

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

コマンドが成功すると、このコマンから接続情報が返されます。

Bitbucket 接続の出力例：

```
{
    "Connection": {
        "ConnectionName": "MyConnection",
```

```
        "ConnectionArn": "arn:aws:codeconnections:us-west-2:account_id:connection/
cdacd948-EXAMPLE",
        "ProviderType": "Bitbucket",
        "OwnerAccountId": "account_id",
        "ConnectionStatus": "AVAILABLE"
    }
}
```

GitHub 接続の出力例：

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

GitHub Enterprise Server Connections の出力例:

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

と接続を共有する AWS アカウント

リソース共有を と使用 AWS RAM して、既存の接続を別の AWS アカウント または組織内のアカウントと共有できます。CodePipeline など、サードパーティーのソース接続用に AWS 管理する のリソースと共有接続を使用できます。

> **Important**
>
> 接続共有は codestar-connections リソースではサポートされていません。これは codeconnectionsリソースでのみサポートされています。

開始する前に:

- との接続が既に作成されている必要があります AWS アカウント。
- リソース共有が有効になっている必要があります。
- 必要なアクセス許可を設定する必要があります。詳細については、「接続共有でサポートされているアクセス許可」を参照してください。

> **Note**
>
> 接続を共有するには、組織所有者であるか、組織内にない場合はリポジトリ所有者である必要があります。共有しているアカウントには、リポジトリへのアクセス許可も必要です。

トピック

- 接続を共有する (コンソール)
- 接続を共有する (CLI)
- 共有接続を表示する (コンソール)
- 共有接続を表示する (CLI)

接続を共有する (コンソール)

コンソールを使用して、共有接続リソースを作成できます。

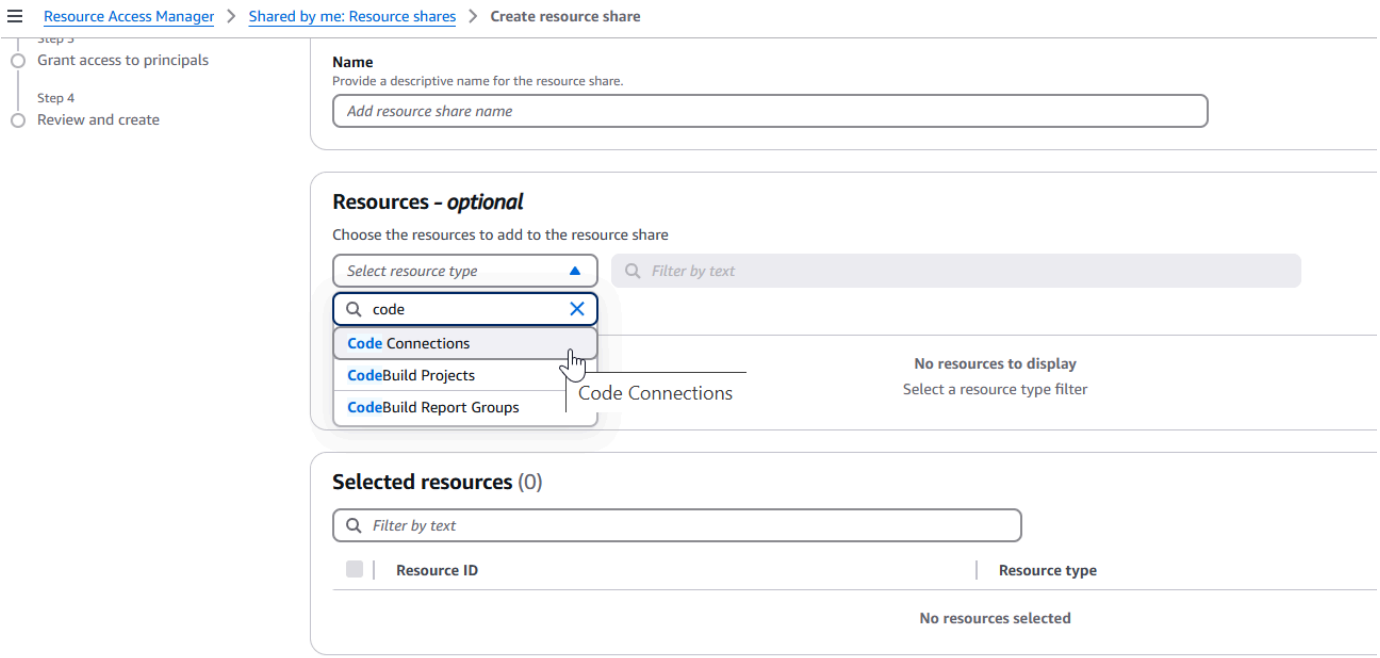
1. AWS マネジメントコンソールにサインインします。

   コンソールの「共有ユーザー : 共有リソース」ページで「リソース共有の作成」を選択します AWS RAM 。
2. AWS RAM リソース共有は特定の AWS リージョンに存在するため、コンソールの右上隅にあるドロップダウンリストから適切な AWS リージョンを選択します。グローバルリソースを含むリ

ソース共有を作成するには、AWS リージョンを米国東部 (バージニア北部) に設定する必要があります。

グローバルリソースの共有の詳細については、「グローバルリソースと比較したリージョンリソースの共有」を参照してください。

3. 作成ページの「名前」に、リソース共有の名前を入力します。リソースで、コード接続を選択します。



4. 接続リソースを選択し、共有するプリンシパルを割り当てます。
5. [作成] を選択します。

接続を共有する (CLI)

AWS Command Line Interface (AWS CLI) を使用して既存の接続を他のアカウントと共有し、所有している、または共有した接続を表示できます。

これを行うには、 create-resource-shareおよび `accept-resource-share-invitation` コマンドを使用します AWS RAM。

接続を共有するには

1. 接続を共有するアカウントでサインインします。
2. ターミナル (Linux/macOS/Unix) またはコマンドプロンプト (Windows) を開きます。 AWS CLI を使用して create-resource-share コマンドを実行し、接続共有`--principals`の `--name`、`--`

resource-arns、 を指定します。この例では、名前は my-shared-resourceで、指定された接続名はリソース ARN MyConnectionにあります。でprincipals、共有している送信先アカウントを指定します。

```
aws ram create-resource-share --name my-shared-resource --resource-
arns connection_ARN --principals destination_account
```

成功した場合、このコマンドは次のような接続 ARN 情報を返します。

```
{
    "resourceShare": {
        "resourceShareArn": "arn:aws:ram:us-west-2:111111111111:resource-
share/4476c27d-8feb-4b21-afe9-7de23EXAMPLE",
        "name": "MyNewResourceShare",
        "owningAccountId": "111111111111",
        "allowExternalPrincipals": true,
        "status": "ACTIVE",
        "creationTime": 1634586271.302,
        "lastUpdatedTime": 1634586271.302
    }
}
```

3. 共有リクエストは、次の手順で説明されているように承諾できます。

送信先アカウントとの接続共有を認証して受け入れるには

次の手順は、同じ組織に属し、Organizations でリソース共有が有効になっている送信先アカウントではオプションです。

1. 招待を受け取る送信先アカウントでサインインします。
2. ターミナル (Linux/macOS/Unix) またはコマンドプロンプト (Windows) を開きます。 AWS CLI を使用して get-resource-share-invitations コマンドを実行します。

```
aws ram get-resource-share-invitations
```

次のステップのリソース共有招待 ARN をキャプチャします。

3. コマンドを実行しaccept-resource-share-invitation、 を指定します--resource-share-invitation-arn。

```
aws ram accept-resource-share-invitation --resource-share-invitation-
arn invitation_ARN
```

成功すると、このコマンドは次の出力を返します。

```
{
    "resourceShareInvitation": {
        "resourceShareInvitationArn": "arn:aws:ram:us-west-2:111111111111:resource-
share-invitation/1e3477be-4a95-46b4-bbe0-c4001EXAMPLE",
        "resourceShareName": "MyResourceShare",
        "resourceShareArn": "arn:aws:ram:us-west-2:111111111111:resource-
share/27d09b4b-5e12-41d1-a4f2-19dedEXAMPLE",
        "senderAccountId": "111111111111",
        "receiverAccountId": "222222222222",
        "invitationTimestamp": "2021-09-22T15:07:35.620000-07:00",
        "status": "ACCEPTED"
    }
}
```

共有接続を表示する (コンソール)

コンソールを使用して、共有接続リソースを表示できます。

1. AWS マネジメントコンソールにサインインします。

   AWS RAM コンソールで共有 : 共有リソースページを開きます。

2. AWS RAM リソース共有は特定の AWS リージョンに存在するため、コンソールの右上隅にあるドロップダウンリストから適切な AWS リージョンを選択します。グローバルリソースを含むリソース共有を表示するには、AWS リージョンを米国東部 (バージニア北部) に設定する必要があります。

   グローバルリソースの共有の詳細については、「グローバルリソースと比較したリージョンリソースの共有」を参照してください。

3. 共有リソース別に以下の情報が表示されます。

   - [Resource ID] (リソース ID) — リソースの ID。リソースの ID を選択してブラウザで新しいタブを開き、ネイティブサービスのコンソールにリソースを表示します。
   - [Resource type] (リソースタイプ) — リソースのタイプ。

- [Last share date] (最終共有日) - リソースが最後に共有された日付。
- [Resource shares] (リソース共有) — リソースを含んでいるリソース共有の数。リソース共有のリストを表示するには、番号を選択します。
- [Principals] (プリンシパル) — リソースにアクセスできるプリンシパルの数。プリンシパルを表示する値を選択します。

共有接続を表示する (CLI)

を使用して AWS CLI 、所有している、または共有した接続を表示できます。

これを行うには、get-resource-shares コマンドを使用します。

共有接続を表示するには

- ターミナル (Linux/macOS/Unix) またはコマンドプロンプト (Windows) を開きます。 AWS CLI を使用して get-resource-shares コマンドを実行します。

  ```
  aws ram get-resource-shares
  ```

  出力は、アカウントのリソース共有のリストを返します。

ホストの使用

インストール済みプロバイダータイプ (GitHub Enterprise Server など) への接続を作成するには、まず AWS マネジメントコンソールを使用してホストを作成します。ホストは、プロバイダーがインストールされているインフラストラクチャを表すために作成するリソースです。次に、そのホストを使用して接続を作成します。詳細については、「接続の使用」を参照してください。

例えば、接続用のホストを作成して、インフラストラクチャを表すためにプロバイダーのサードパーティーアプリを登録できるようにします。プロバイダータイプに対してホストを 1 つ作成ます。そのプロバイダータイプへのすべての接続がそのホストを使用します。

コンソールを使用してインストール済みプロバイダータイプ (GitHub Enterprise Server など) への接続を作成すると、コンソールがホストリソースを作成します。

トピック

- ホストを作成する
- 保留中のホストをセットアップする

- ホストを一覧表示
- ホストを編集する
- ホストを削除する
- ホストの詳細の表示

ホストを作成する

AWS マネジメントコンソール または AWS Command Line Interface (AWS CLI) を使用して、インフラストラクチャにインストールされているサードパーティーのコードリポジトリへの接続を作成できます。例えば、GitHub Enterprise Server を Amazon EC2 インスタンス上で仮想マシンとして実行しているとします。GitHub Enterprise Server への接続を作成する前に、接続に使用するホストを作成します。

インストール済みプロバイダー用のホスト作成ワークフローの概要については、「ホストを作成または更新するワークフロー」を参照してください。

開始する前に:

- (オプション) VPC を使用してホストを作成する場合は、ネットワークまたは仮想プライベートクラウド (VPC) をあらかじめ作成しておく必要があります。
- インスタンスをあらかじめ作成しておく必要があります。VPC に接続するときは、ホストを VPC で起動しておく必要があります。

> **Note**
>
> 各 VPC は、一度に 1 つのホストにのみ関連付けることができます。

オプションで VPC を使用してホストを設定できます。ホストリソース用のネットワークおよび VPC 設定の詳細については、「(オプション) 前提条件: 接続用のネットワーク設定または Amazon VPC 設定」および「ホストの VPC 設定のトラブルシューティング」を参照してください。

コンソールを使用してホストを作成し、GitHub Enterprise Server への接続を作成するには、「GitHub Enterprise Server 接続を作成する (コンソール)」を参照してください。コンソールでホストが作成されます。

コンソールを使用してホストを作成し、GitHub セルフマネージドへの接続を作成するには、「GitLab セルフマネージドへの接続を作成する」を参照してください。コンソールでホストが作成されます。

(オプション) 前提条件: 接続用のネットワーク設定または Amazon VPC 設定

インフラストラクチャにネットワーク接続が設定されている場合は、このセクションをスキップできます。

ホストに VPC でのみアクセスできる場合は、続行する前に、これらの VPC 要件に従ってください。

VPC の要件

オプションで VPC を使用してホストを作成することもできます。以下は、インストール用に設定した VPC に応じた、一般的な VPC 要件を示します。

- パブリックサブネットとプライベートサブネットを使用してパブリック VPC を構成できます。優先 CIDR ブロックまたはサブネットがない場合は、 AWS アカウント にデフォルトの VPC を使用できます。
- プライベート VPC を設定していて、非公開認証局を使用して TLS 検証を実行するように GitHub Enterprise Server インスタンスを設定している場合は、ホストリソースに TLS 証明書を提供する必要があります。
- 接続によってホストが作成されると、ウェブフックの VPC エンドポイント (PrivateLink) が自動的に作成されます。詳細については、「AWS CodeConnections およびインターフェイス VPC エンドポイント (AWS PrivateLink)」を参照してください。
- セキュリティグループの設定
  - ホストの作成時に使用されるセキュリティグループには、ネットワークインターフェイスが GitHub Enterprise Server インスタンスに接続できるようにするインバウンドルールとアウトバウンドルールが必要です。
  - GitHub Enterprise Server インスタンス (ホスト設定の一部ではない) にアタッチされたセキュリティグループには、接続によって作成されたネットワークインターフェイスからのインバウンドアクセスとアウトバウンドアクセスが必要です。
- VPC サブネットは、リージョン内の異なるアベイラビリティーゾーンに存在している必要があります。アベイラビリティーゾーンとは、他のアベイラビリティーゾーンで発生した障害から切り離すために作られた場所です。各サブネットが完全に 1 つのアベイラビリティーゾーン内に含まれている必要があり、1 つのサブネットが複数のゾーンに、またがることはできません。

VPC とサブネットの使用方法の詳細については、Amazon VPC ユーザーガイド の「IPv4 用の VPC とサブネットのサイズ設定」を参照してください。

ホストセットアップ用に提供する VPC 情報

次のステップで接続用のホストリソースを作成するときは、以下を提供する必要があります。

- VPC ID: GitHub Enterprise Server インスタンスがインストールされているサーバーの VPC、または VPN または Direct Connect を介してインストールされた GitHub Enterprise Server インスタンスにアクセスできる VPC の ID。
- サブネット ID: GitHub Enterprise Server インスタンスがインストールされているサーバーのサブネット、または VPN または Direct Connect を介してインストールされた GitHub Enterprise Server インスタンスにアクセスできるサブネットの ID。
- セキュリティグループ: GitHub Enterprise Server インスタンスがインストールされているサーバーのセキュリティグループ、または VPN または Direct Connect を介してインストールされた GitHub Enterprise Server インスタンスにアクセスできるセキュリティグループ。
- エンドポイント: サーバーエンドポイントを準備して、次のステップに進みます。

VPC またはホスト接続のトラブルシューティングなどの詳細については、「ホストの VPC 設定のトラブルシューティング」を参照してください。

アクセス許可の要件

ホスト作成プロセスの一環として、 はユーザーに代わってネットワークリソース AWS CodeConnections を作成し、VPC 接続を容易にします。これには、ホストからデータをクエリ AWS CodeConnections するための のネットワークインターフェイスと、ホストがウェブフックを介して接続にイベントデータを送信するための VPC エンドポイントまたは PrivateLink が含まれます。これらのネットワークリソースを作成できるようにするには、ホストを作成するロールに次のアクセス許可があることを確認してください。

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

```
ec2:DescribeVpcEndpoints
```

VPC 内のアクセス許可またはホスト接続のトラブルシューティングの詳細については、「ホストの VPC 設定のトラブルシューティング」を参照してください。

ウェブフック VPC エンドポイントの詳細については、「AWS CodeConnections およびインターフェイス VPC エンドポイント (AWS PrivateLink)」を参照してください。

トピック

- 接続用のホストを作成する (コンソール)
- 接続用のホストを作成する (CLI)

接続用のホストを作成する (コンソール)

GitHub Enterprise Server や GitLab セルフマネージドなど、インストールの接続では、ホストを使用して、サードパーティーのプロバイダーがインストールされているインフラストラクチャのエンドポイントを表します。

> **Note**
>
> 2024 年 7 月 1 日以降、コンソールはリソース ARN codeconnectionsに との接続を作成します。両方のサービスプレフィックスを持つリソースは、コンソールに引き続き表示されます。

VPC でホストをセットアップする際の考慮事項については、「GitLab セルフマネージドへの接続を作成する」を参照してください。

コンソールを使用してホストを作成し、GitHub Enterprise Server への接続を作成するには、「GitHub Enterprise Server 接続を作成する (コンソール)」を参照してください。コンソールでホストが作成されます。

コンソールを使用してホストを作成し、GitHub セルフマネージドへの接続を作成するには、「GitLab セルフマネージドへの接続を作成する」を参照してください。コンソールでホストが作成されます。

> **Note**
>
> ホストは、GitHub Enterprise Server または GitLab セルフマネージドアカウントごとに 1 回だけ作成します。特定の GitHub Enterprise Server または GitLab セルフマネージドアカウントへの接続はすべて、同じホストを使用します。

接続用のホストを作成する (CLI)

AWS Command Line Interface (AWS CLI) を使用して、インストールされた接続用のホストを作成できます。

> **Note**
>
> ホストは、GitHub Enterprise Server アカウントごとに 1 回だけ作成しまう。特定の GitHub Enterprise Server アカウントへの接続はすべて、同じホストを使用します。

ホストを使用して、サードパーティーのプロバイダがインストールされているインフラストラクチャのエンドポイントを表します。CLI を使用してホストを作成するには、create-host コマンドを実行します。ホストの作成が完了すると、ホストのステータスが Pending (保留中) になります。次に、ホストを設定して、ホストのステータスが Available (使用可能) に移行します。ホストが使用可能になったら、接続を作成する手順を完了します。

> **Important**
>
> を通じて作成されたホスト AWS CLI は、デフォルトで `Pending`ステータスになります。CLI でホストを作成後、コンソールでホストを設定し、ステータスを `Available` にします。

コンソールを使用してホストを作成し、GitHub Enterprise Server への接続を作成するには、「GitHub Enterprise Server 接続を作成する (コンソール)」を参照してください。コンソールでホストが作成されます。

コンソールを使用してホストを作成し、GitHub セルフマネージドへの接続を作成するには、「GitLab セルフマネージドへの接続を作成する」を参照してください。コンソールでホストが作成されます。

保留中のホストをセットアップする

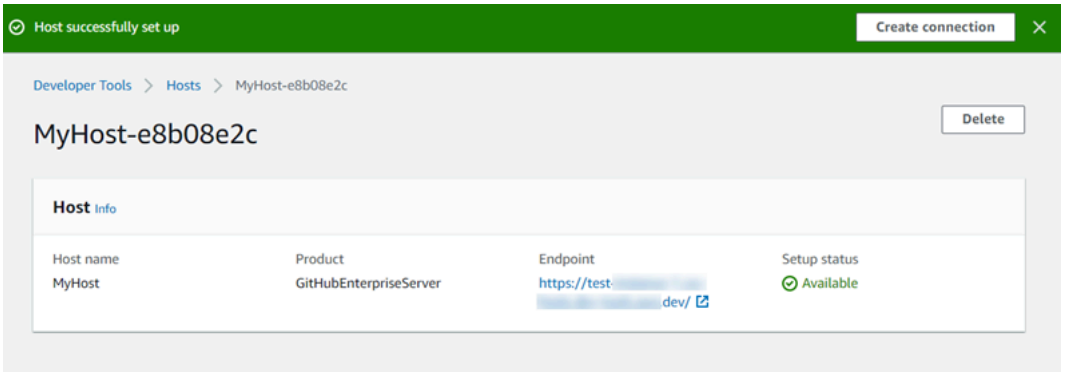
AWS Command Line Interface (AWS CLI) または SDK を使用して作成されたホストは、デフォルトで Pendingステータスです。コンソールまたは SDK との接続を作成したら、 コンソールを使用してホストをセットアップし AWS CLI、ステータスを にしますAvailable。

予めホストを作成しておく必要があります。詳細については、「Create a host」を参照してください。

保留中のホストをセットアップするには

ホストが作成されると、ステータスが Pending (保留中) になります。ホストをPending から Available に移行するには、次の手順を実行します。このプロセスは、サードパーティープロバイダーとのハンドシェイクを実行して、 AWS 接続アプリケーションをホストに登録します。

1. デ AWS ベロッパーツールコンソールでホストのステータスが保留中になったら、ホストのセットアップを選択します。
2. GitLab セルフマネージド用のホストを作成する場合は、[セットアップ] ページが表示されます。[個人アクセストークンの提供] で、GitLab PAT に、api というスコープダウンされたアクセス許可のみを指定します。
3. GitHub Enterprise Server ログインページなどのサードパーティーのインストール済みプロバイダーのログインページでプロンプトが表示されたら、アカウントの認証情報を使用してログインします。
4. アプリのインストールページの [GitHub App name] (GitHub アプリ名) に、ホストにインストールするアプリの名前を入力します。Create GitHub App (GitHub アプリの作成) を選択します。
5. ホストが正常に登録されると、ホストの詳細ページが表示され、ホストのステータスが Available (使用可能) になります。



6. ホストが使用可能になった後も、接続の作成を続行できます。成功バナーで、[Create connection] (接続を作成する) を選択します。[Create a connection] (接続を作成する) の手順を完了します。

ホストを一覧表示

開発者用ツールコンソールまたは AWS Command Line Interface (AWS CLI) 内の list-connections コマンドを使用して、アカウント内の接続のリストを表示できます。

ホストを一覧表示 (コンソール)

ホストを一覧表示するには

1. https://console.aws.amazon.com/codesuite/settings/connections でデベロッパーツールコンソールを開きます。
2. [Hosts] (ホスト) タブを選択します。ホストの名前、ステータス、および ARN を表示します。

ホストを一覧表示 (CLI)

を使用して AWS CLI 、インストールされているサードパーティープロバイダー接続のホストを一覧表示できます。

これを行うには、list-hosts コマンドを使用します。

ホストを一覧表示するには

- ターミナル (Linux、macOS、または Unix) またはコマンドプロンプト (Windows) を開き、AWS CLI を使用してlist-hostsコマンドを実行します。

```
aws codeconnections list-hosts
```

このコマンドで、以下の出力が返ります。

```
{
    "Hosts": [
        {
            "Name": "My-Host",
            "HostArn": "arn:aws:codeconnections:us-west-2:account_id:host/My-
Host-28aef605",
```

```
            "ProviderType": "GitHubEnterpriseServer",
            "ProviderEndpoint": "https://my-instance.test.dev",
            "Status": "AVAILABLE"
        }
    ]
}
```

ホストを編集する

Pending ステータスのホストのホスト設定を編集できます。ホスト名、URL、または VPC 設定を編集できます。

同じ URL を複数のホストに使用することはできません。

> **Note**
>
> VPC でホストをセットアップする際の考慮事項については、「(オプション) 前提条件: 接続用のネットワーク設定または Amazon VPC 設定」を参照してください。

ホストを編集するには

1. https://console.aws.amazon.com/codesuite/settings/connections でデベロッパーツールコンソールを開きます。
2. [設定] > [接続] を選択します。
3. [Hosts] (ホスト) タブを選択します。

   AWS アカウントに関連付けられ、選択した AWS リージョンで作成されたホストが表示されます。
4. ホスト名を編集するには、[Name] (名前) に新しい値を入力します
5. ホストエンドポイントを編集するには、[URL] に新しい値を入力します。
6. ホスト VPC 設定を編集するには、[VPC ID] に新しい値を入力します。
7. [Edit host] (ホストを編集) を選択します。
8. 更新された設定が表示されます。[Set up Pending host] (保留中のホストの設定) を選択します。

ホストを削除する

デベロッパーツールコンソールまたは AWS Command Line Interface (AWS CLI) の delete-host コマンドを使用して、ホストを削除できます。

トピック

ホストの削除 (コンソール)

ホストを削除するには

1. https://console.aws.amazon.com/codesuite/settings/connections でデベロッパーツールコンソールを開きます。
2. [Hosts] (ホスト) タブを選択します。[Name] (名前) で、削除するホストの名前を選択します。
3. [削除] を選択します。
4. フィールドに「**delete**」と入力して確認し、[Delete (削除)] を選択します。

> **Important**
> このアクションを元に戻すことはできません。

ホストの削除 (CLI)

AWS Command Line Interface （ AWS CLI) を使用してホストを削除できます。

これを行うには、delete-host コマンドを使用します。

> **Important**
> ホストを削除する前に、ホストに関連付けられたすべての接続を削除する必要があります。コマンドを実行すると、ホストは削除されます。確認のダイアログボックスは表示されません。

ホストを削除するには

- ターミナル (Linux/macOS/Unix) またはコマンドプロンプト (Windows) を開きます。を使用して delete-host コマンド AWS CLI を実行し、削除するホストの Amazon リソースネーム (ARN) を指定します。

```
aws codeconnections delete-host --host-arn "arn:aws:codeconnections:us-
west-2:account_id:host/My-Host-28aef605"
```

このコマンドは何も返しません。

ホストの詳細の表示

デベロッパーツールコンソールまたは AWS Command Line Interface (AWS CLI) の get-host コマンドを使用して、ホストの詳細を表示します。

ホストの詳細を表示するには (コンソール)

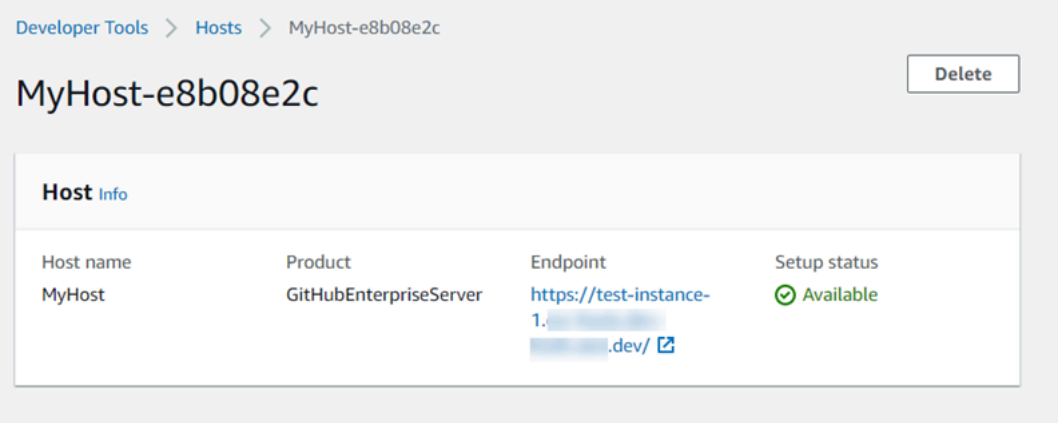
1. AWS マネジメントコンソール にサインインして、https://console.aws.amazon.com/codesuite/settings/connections でデベロッパーツールコンソールを開きます。
2. [設定] > [接続] を選択して、次に [ホスト] タブを選択します。
3. 表示するホストの横にあるボタンを選択して、[View event details] (イベント詳細を表示) をクリックします。
4. ホストに関する次の情報が表示されます。

   - ホスト名。
   - 接続のプロバイダータイプ。
   - プロバイダーがインストールされているインフラストラクチャのエンドポイント。
   - ホストの設定ステータス。接続の準備が整ったホストのステータスは、Available (使用可能) になります。ホストは作成されたが、セットアップが完了しなかった場合は、ホストのステータスが異なる可能性があります。

     以下のステータスがあります。

     - PENDING - ホストは、作成を完了し、ホストにプロバイダーアプリを登録してセットアップを開始する準備ができています。
     - AVIAL - ホストは、作成とセットアップを完了し、接続で使用できます。

- ERROR - ホストの作成または登録中にエラーが発生しました。
- VPC_CONFIG_VPC_INITIALIZING - ホストの VPC 設定を作成中です。
- VPC_CONFIG_VPC_FAILED_INITIALIZATION - ホストの VPC 設定が検出され、エラーが発生して失敗しました。
- VPC_CONFIG_VPC_AVAILABLE - ホストの VPC 設定はセットアップが完了し、使用可能です。
- VPC_CONFIG_VPC_DELETING - ホストの VPC 設定を削除中です。



5. ホストを削除するには、[Delete] (削除) を選択します。
6. ホストのステータスが Pending (保留中) の場合、セットアップを完了するにはホストの設定を選択します。詳細については、Set up a pending host (保留中のホストをセットアップする) を参照してください。

ホストの詳細を表示するには (CLI)

- ターミナル (Linux、macOS、または Unix) またはコマンドプロンプト (Windows) を開き、AWS CLI を使用してget-hostコマンドを実行し、詳細を表示するホストの Amazon リソースネーム (ARN) を指定します。

```
aws codeconnections get-host --host-arn arn:aws:codeconnections:us-
west-2:account_id:host/My-Host-28aef605
```

このコマンドで、以下の出力が返ります。

```
{
    "Name": "MyHost",
```

```
    "Status": "AVAILABLE",
    "ProviderType": "GitHubEnterpriseServer",
    "ProviderEndpoint": "https://test-instance-1.dev/"
}
```

リンクされたリポジトリの同期設定を操作する

In AWS CodeConnections では、接続を使用してGitHub、Bitbucket Cloud、GitHub Enterprise Server、GitLab などのサードパーティーリポジトリに AWS リソースを関連付けます。CFN_STACK_SYNC 同期タイプを使用すると、同期設定を作成できます。これにより、 は AWS Git リポジトリのコンテンツを同期して、指定された AWS リソースを更新できます。 は、Git 同期を使用して同期するリンクされたリポジトリ内のテンプレートとパラメータファイルを管理できるように、 接続と CloudFormation 統合します。

接続を作成したら、接続 CLI または CloudFormation コンソールを使用してリポジトリリンクと同期設定を作成できます。

- リポジトリリンク: リポジトリリンクは、接続と外部の Git リポジトリとの関連付けを作成します。リポジトリリンクにより、Git 同期は指定された Git リポジトリ内のファイルへの変更をモニタリングして同期できます。
- 同期設定: 同期設定を使用して Git リポジトリからコンテンツを同期し、指定された AWS リソースを更新します。

詳細については、AWS CodeConnections API リファレンス」を参照してください。

CloudFormation コンソールを使用して CloudFormation スタックの同期設定を作成するチュートリアルについては、CloudFormation ユーザーガイド」のCloudFormation 「Git 同期の使用」を参照してください。

トピック

- リポジトリリンクを操作する
- 同期設定を使用する

リポジトリリンクを操作する

リポジトリリンクは、接続と外部の Git リポジトリとの関連付けを作成します。リポジトリリンクを使用すると、Git 同期は指定された Git リポジトリ内のファイルへの変更をモニタリングし、CloudFormation スタックに同期できます。

リポジトリリンクの詳細については、AWS CodeConnections API リファレンスを参照してください。

トピック

レポジトリリンクを作成する

AWS Command Line Interface (AWS CLI) の create-repository-link コマンドを使用して、接続と同期する外部リポジトリ間のリンクを作成できます。

リポジトリリンクを作成するには、GitHub などのサードパーティープロバイダーを使用して外部リポジトリを事前に作成しておく必要があります。

レポジトリリンクを作成するには

1. ターミナル (Linux/macOS/Unix) またはコマンドプロンプト (Windows) を開きます。 AWS CLI を使用して create-repository-link コマンドを実行します。関連する接続の ARN、所有者 ID、およびリポジトリ名を指定します。

```
aws codeconnections create-repository-link --connection-arn
 arn:aws:codeconnections:us-east-1:account_id:connection/001f5be2-a661-46a4-
b96b-4d277cac8b6e --owner-id account_id --repository-name MyRepo
```

2. このコマンドで、以下の出力が返ります。

```
{
    "RepositoryLinkInfo": {
```

```
        "ConnectionArn": "arn:aws:codeconnections:us-east-1:account_id:connection/
aEXAMPLE-8aad-4d5d-8878-dfcab0bc441f",
        "OwnerId": "account_id",
        "ProviderType": "GitHub",
        "RepositoryLinkArn": "arn:aws:codeconnections:us-
east-1:account_id:repository-link/be8f2017-b016-4a77-87b4-608054f70e77",
        "RepositoryLinkId": "be8f2017-b016-4a77-87b4-608054f70e77",
        "RepositoryName": "MyRepo",
        "Tags": []
    }
}
```

レポジトリリンクを更新する

AWS Command Line Interface (AWS CLI) の update-repository-link コマンドを使用して、指定されたリポジトリリンクを更新できます。

リポジトリリンクの次の情報を更新できます。

- `--connection-arn`
- `--owner-id`
- `--repository-name`

リポジトリに関連付けられている接続を変更したいときに、リポジトリリンクを更新できます。別の接続を使用するには、接続 ARN を指定する必要があります。接続 ARN を表示する手順については、「接続の詳細を表示する」を参照してください。

レポジトリリンクを更新するには

1. ターミナル (Linux/macOS/Unix) またはコマンドプロンプト (Windows) を開きます。 AWS CLI を使用して update-repository-link コマンドを実行し、リポジトリリンクに対して更新する値を指定します。例えば、以下のコマンドはリポジトリリンク ID に関連付けられた接続を更新します。新しい接続 ARN を `--connection` パラメータで指定します。

```
aws codestar-connections update-repository-link --repository-link-id
 6053346f-8a33-4edb-9397-10394b695173 --connection-arn arn:aws:codestar-
connections:us-east-1:account_id:connection/aEXAMPLE-f055-4843-adef-4ceaefcb2167
```

2. このコマンドで、以下の出力が返ります。

```
{
    "RepositoryLinkInfo": {
        "ConnectionArn": "arn:aws:codestar-connections:us-
east-1:account_id:connection/aEXAMPLE-f055-4843-adef-4ceaefcb2167",
        "OwnerId": "owner_id",
        "ProviderType": "GitHub",
        "RepositoryLinkArn": "arn:aws:codestar-connections:us-
east-1:account_id:repository-link/6053346f-8a33-4edb-9397-10394b695173",
        "RepositoryLinkId": "6053346f-8a33-4edb-9397-10394b695173",
        "RepositoryName": "MyRepo",
        "Tags": []
    }
}
```

リポジトリリンクを一覧表示する

AWS Command Line Interface (AWS CLI) の list-repository-links コマンドを使用して、アカウントのリポジトリリンクを一覧表示できます。

リポジトリリンクを一覧表示するには

1. ターミナル (Linux/macOS/Unix) またはコマンドプロンプト (Windows) を開きます。 AWS CLI を使用して list-repository-links コマンドを実行します。

```
aws codeconnections list-repository-links
```

2. このコマンドで、以下の出力が返ります。

```
{
    "RepositoryLinks": [
        {
            "ConnectionArn": "arn:aws:codestar-connections:us-
east-1:account_id:connection/001f5be2-a661-46a4-b96b-4d277cac8b6e",
            "OwnerId": "owner_id",
            "ProviderType": "GitHub",
            "RepositoryLinkArn": "arn:aws:codestar-connections:us-
east-1:account_id:repository-link/6053346f-8a33-4edb-9397-10394b695173",
            "RepositoryLinkId": "6053346f-8a33-4edb-9397-10394b695173",
            "RepositoryName": "MyRepo",
            "Tags": []
        }
```

```
    ]
}
```

リポジトリリンクを削除する

AWS Command Line Interface (AWS CLI) の delete-repository-link コマンドを使用して、リポジトリリンクを削除できます。

リポジトリリンクを削除する前に、リポジトリリンクに関連付けられた同期設定をすべて削除する必要があります。

> **Important**
>
> コマンドを実行すると、レポジトリリンクは削除されます。確認のダイアログボックスは表示されません。新しいレポジトリリンクを作成することはできますが、Amazon リソースネーム (ARN) は再利用されません。

リポジトリリンクを削除するには

- ターミナル (Linux/macOS/Unix) またはコマンドプロンプト (Windows) を開きます。 AWS CLI を使用して delete-repository-link コマンドを実行し、削除するリポジトリリンクの ID を指定します。

  ```
  aws codeconnections delete-repository-link --repository-link-id
   6053346f-8a33-4edb-9397-10394b695173
  ```

  このコマンドは何も返しません。

リポジトリリンクの詳細を表示する

AWS Command Line Interface (AWS CLI) の get-repository-link コマンドを使用して、リポジトリリンクの詳細を表示できます。

リポジトリリンクの詳細を表示するには

1. ターミナル (Linux/macOS/Unix) またはコマンドプロンプト (Windows) を開きます。 AWS CLI を使用して get-repository-link コマンドを実行し、リポジトリリンク ID を指定します。

```
aws codestar-connections get-repository-link --repository-link-id
 6053346f-8a33-4edb-9397-10394b695173
```

2. このコマンドで、以下の出力が返ります。

```
{
    "RepositoryLinkInfo": {
        "ConnectionArn": "arn:aws:codestar-connections:us-
east-1:account_id:connection/aEXAMPLE-8aad-4d5d-8878-dfcab0bc441f",
        "OwnerId": "owner_id",
        "ProviderType": "GitHub",
        "RepositoryLinkArn": "arn:aws:codestar-connections:us-
east-1:account_id:repository-link/be8f2017-b016-4a77-87b4-608054f70e77",
        "RepositoryLinkId": "6053346f-8a33-4edb-9397-10394b695173",
        "RepositoryName": "MyRepo",
        "Tags": []
    }
}
```

同期設定を使用する

同期設定により、指定したリポジトリと接続が関連付けられます。同期設定を使用して Git リポジトリのコンテンツを同期し、指定された AWS リソースを更新します。

接続の詳細については、AWS CodeConnections API リファレンスを参照してください。

トピック

- 同期設定を作成する
- 同期設定を更新する
- 同期設定を一覧表示する
- 同期設定を削除する
- 同期設定の詳細を表示する

同期設定を作成する

AWS Command Line Interface (AWS CLI) の create-repository-link コマンドを使用して、接続と同期する外部リポジトリ間のリンクを作成できます。

同期設定を作成する前に、接続とサードパーティーのリポジトリとの間にリポジトリリンクを作成しておく必要があります。

同期設定を作成するには

1. ターミナル (Linux/macOS/Unix) またはコマンドプロンプト (Windows) を開きます。 AWS CLI を使用して create-repository-link コマンドを実行します。関連する接続の ARN、所有者 ID、およびリポジトリ名を指定します。次のコマンドは、 CloudFormation内のリソースの同期タイプを使用して同期設定を作成します。また、リポジトリ内のリポジトリブランチと設定ファイルも指定します。この例では、リソースは **mystack** という名前のスタックです。

```
aws codeconnections create-sync-configuration --branch main --config-file filename
 --repository-link-id be8f2017-b016-4a77-87b4-608054f70e77 --resource-name mystack
 --role-arn arn:aws:iam::account_id:role/myrole --sync-type CFN_STACK_SYNC
```

2. このコマンドで、以下の出力が返ります。

```
{
    "SyncConfiguration": {
        "Branch": "main",
        "ConfigFile": "filename",
        "OwnerId": "account_id",
        "ProviderType": "GitHub",
        "RepositoryLinkId": "be8f2017-b016-4a77-87b4-608054f70e77",
        "RepositoryName": "MyRepo",
        "ResourceName": "mystack",
        "RoleArn": "arn:aws:iam::account_id:role/myrole",
        "SyncType": "CFN_STACK_SYNC"
    }
```

同期設定を更新する

AWS Command Line Interface (AWS CLI) の update-sync-configuration コマンドを使用して、指定された同期設定を更新できます。

同期設定に関する次の情報を更新できます。

- `--branch`
- `--config-file`
- `--repository-link-id`

- `--resource-name`
- `--role-arn`

同期設定を更新するには

1. ターミナル (Linux/macOS/Unix) またはコマンドプロンプト (Windows) を開きます。 AWS CLI を使用して update-sync-configuration コマンドを実行し、更新する値とリソース名と同期タイプを指定します。例えば、次のコマンドは、同期設定に関連付けられているブランチ名を `--branch` パラメータで更新します。

```
aws codeconnections update-sync-configuration --sync-type CFN_STACK_SYNC --
resource-name mystack --branch feature-branch
```

2. このコマンドで、以下の出力が返ります。

```
{
    "SyncConfiguration": {
        "Branch": "feature-branch",
        "ConfigFile": "filename.yaml",
        "OwnerId": "owner_id",
        "ProviderType": "GitHub",
        "RepositoryLinkId": "6053346f-8a33-4edb-9397-10394b695173",
        "RepositoryName": "MyRepo",
        "ResourceName": "mystack",
        "RoleArn": "arn:aws:iam::account_id:role/myrole",
        "SyncType": "CFN_STACK_SYNC"
    }
```

同期設定を一覧表示する

AWS Command Line Interface (AWS CLI) の list-sync-configurations のコマンドを使用して、アカウントのリポジトリリンクを一覧表示できます。

リポジトリリンクを一覧表示するには

1. ターミナル (Linux/macOS/Unix) またはコマンドプロンプト (Windows) を開きます。 AWS CLI を使用して list-sync-configurations コマンドを実行し、同期タイプとリポジトリリンク ID を指定します。

```
aws codeconnections list-sync-configurations --repository-link-id
 6053346f-8a33-4edb-9397-10394b695173  --sync-type CFN_STACK_SYNC
```

2. このコマンドで、以下の出力が返ります。

```
{
    "SyncConfigurations": [
        {
            "Branch": "main",
            "ConfigFile": "filename.yaml",
            "OwnerId": "owner_id",
            "ProviderType": "GitHub",
            "RepositoryLinkId": "6053346f-8a33-4edb-9397-10394b695173",
            "RepositoryName": "MyRepo",
            "ResourceName": "mystack",
            "RoleArn": "arn:aws:iam::account_id:role/myrole",
            "SyncType": "CFN_STACK_SYNC"
        }
    ]
}
```

同期設定を削除する

AWS Command Line Interface (AWS CLI) の delete-sync-configuration コマンドを使用して、同期設定を削除できます。

> **Important**
>
> コマンドを実行すると、同期設定は削除されます。確認のダイアログボックスは表示されません。新しい同期設定を作成することはできますが、Amazon リソースネーム (ARN) は再利用されません。

同期設定を削除するには

- ターミナル (Linux/macOS/Unix) またはコマンドプロンプト (Windows) を開きます。 AWS CLI を使用して delete-sync-configuration コマンドを実行し、削除する同期設定の同期タイプとリソース名を指定します。

```
aws codeconnections delete-sync-configuration --sync-type CFN_STACK_SYNC --
resource-name mystack
```

このコマンドは何も返しません。

同期設定の詳細を表示する

AWS Command Line Interface (AWS CLI) の get-sync-configuration コマンドを使用して、同期設定の詳細を表示できます。

同期設定の詳細を表示するには

1. ターミナル (Linux/macOS/Unix) またはコマンドプロンプト (Windows) を開きます。 AWS CLI を使用して get-sync-configuration コマンドを実行し、リポジトリリンク ID を指定します。

```
aws codeconnections get-sync-configuration --sync-type CFN_STACK_SYNC --resource-
name mystack
```

2. このコマンドで、以下の出力が返ります。

```
{
    "SyncConfiguration": {
        "Branch": "main",
        "ConfigFile": "filename",
        "OwnerId": "owner_id",
        "ProviderType": "GitHub",
        "RepositoryLinkId": "be8f2017-b016-4a77-87b4-608054f70e77",
        "RepositoryName": "MyRepo",
        "ResourceName": "mystack",
        "RoleArn": "arn:aws:iam::account_id:role/myrole",
        "SyncType": "CFN_STACK_SYNC"
    }
}
```

を使用した Logging AWS CodeConnections API コール AWS CloudTrail

AWS CodeConnections は、ユーザー AWS CloudTrail、ロール、または 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。CloudTrail は、 のすべての API コールをイベント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、開発者向けツール

コンソールからの呼び出しと、 AWS CodeConnections API オペレーションへのコードの呼び出しが含まれます。

証跡を作成すると、通知のイベントを含め、CloudTrail イベントを Amazon Simple Storage Service (Amazon S3) バケットに継続的に配信できるようになります。証跡を設定しない場合でも、CloudTrail コンソールの [Event history (イベント履歴)] で最新のイベントを表示できます。CloudTrail が収集した情報を使用して、 AWS CodeConnectionsに対して行われたリクエスト、リクエスト元の IP アドレス、リクエスト者、リクエスト日時、および追加の詳細を確認できます。

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 CodeConnections 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。アクティビティが発生すると AWS CodeConnections、そのアクティビティはイベント履歴の他の AWS サービスイベントとともに CloudTrail 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、「AWS CloudTrail ユーザーガイド」の「Viewing events with CloudTrail event history」(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 アカウント内のイベントの継続的な記録については AWS CodeConnections、証跡を作成します。証跡により、CloudTrail はログファイルを Amazon S3 バケットに配信できます。デフォルトでは、コンソールで証跡を作成するときに、証跡がすべての 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記録し、指定した Amazon S3 バケットにログファイルを配信します。さらに、CloudTrail ログで収集されたイベントデータをさらに分析して処理するように他の AWS サービスを設定できます。

詳細については、『AWS CloudTrail ユーザーガイド:』の以下のトピックを参照してください。

- 証跡作成の概要
- CloudTrail がサポートされているサービスと統合
- 「CloudTrail の Amazon SNS 通知の設定」
- CloudTrail ログ ファイルを複数のリージョンから受け取る
- 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 CodeConnections アクションは CloudTrail によってログに記録され、AWS CodeConnections API リファレンスに記載されています。例え

ば、CreateConnection、DeleteConnection、GetConnection 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、誰がリクエストを生成したかという情報が含まれます。アイデンティティ情報は、以下を判別するのに役立ちます。

- リクエストが、ルートと他の IAM 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テンポラリ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。

ログファイルエントリの理解

「トレイル」は、指定した Simple Storage Service (Amazon S3) バケットにイベントをログファイルとして配信するように設定できます。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、任意の出典からの単一のリクエストを表し、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に関する情報が含まれます。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。

CreateConnection の例

以下の例は、CreateConnection アクションを示す CloudTrail ログエントリです。


```
{
    "EventId": "b4374fde-c544-4d43-b511-7d899568e55a",
    "EventName": "CreateConnection",
    "ReadOnly": "false",
    "AccessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "EventTime": "2024-01-09T15:13:46-08:00",
    "EventSource": "codeconnections.amazonaws.com",
    "Username": "Mary_Major",
    "Resources": [],
    "CloudTrailEvent": {
        "eventVersion": "1.08",
        "userIdentity": {
            "type": "AssumedRole",
            "principalId": "AIDACKCEVSQ6C2EXAMPLE",
            "arn": "arn:aws:sts::123456789012:assumed-role/Admin/Mary_Major",
```

```
            "accountId": "123456789012",
            "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
            "sessionContext": {
                "sessionIssuer": {
                    "type": "Role",
                    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                    "arn": "arn:aws:iam::123456789012:user/Mary_Major",
                    "accountId": "123456789012",
                    "userName": "Admin"
                },
                "webIdFederationData": {},
                "attributes": {
                    "creationDate": "2024-01-09T23:03:08Z",
                    "mfaAuthenticated": "false"
                }
            }
        },
        "eventTime": "2024-01-09T23:13:46Z",
        "eventSource": "codeconnections.amazonaws.com",
        "eventName": "CreateConnection",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "IP",
        "userAgent": "aws-cli/2.13.30 Python/3.11.6 Darwin/23.2.0 exe/x86_64 prompt/off
 command/codeconnections.create-connection",
        "requestParameters": {
            "providerType": "GitHub",
            "connectionName": "my-connection"
        },
        "responseElements": {
            "connectionArn": "arn:aws:codeconnections:us-
east-1:123456789012:connection/df03df74-8e05-45cf-b420-b39e389dd264"
        },
        "requestID": "57640a88-97b7-481d-9665-cfd79a681379",
        "eventID": "b4374fde-c544-4d43-b511-7d899568e55a",
        "readOnly": false,
        "eventType": "AwsApiCall",
        "managementEvent": true,
        "recipientAccountId": "123456789012",
        "eventCategory": "Management",
        "tlsDetails": {
            "clientProvidedHostHeader": "api.us-east-1.codeconnections.aws.dev"
        }
    }
```

```
}
```

CreateHost の例

以下の例は、CreateHost アクションを示す CloudTrail ログエントリです。

```
{
    "EventId": "af4ce349-9f21-43fb-8003-267fbf9b1a93",
    "EventName": "CreateHost",
    "ReadOnly": "false",
    "AccessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "EventTime": "2024-01-11T12:43:06-08:00",
    "EventSource": "codeconnections.amazonaws.com",
    "Username": "Mary_Major",
    "Resources": [],
    "CloudTrailEvent": {
        "eventVersion": "1.08",
        "userIdentity": {
            "type": "AssumedRole",
            "principalId": "AIDACKCEVSQ6C2EXAMPLE",
            "arn": "arn:aws:sts::123456789012:assumed-role/Admin/Mary_Major",
            "accountId": "123456789012",
            "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
            "sessionContext": {
                "sessionIssuer": {
                    "type": "Role",
                    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                    "arn": "arn:aws:sts::123456789012:assumed-role/Admin/Mary_Major",
                    "accountId": "123456789012",
                    "userName": "Admin"
                },
                "webIdFederationData": {},
                "attributes": {
                    "creationDate": "2024-01-11T20:09:35Z",
                    "mfaAuthenticated": "false"
                }
            }
        },
        "eventTime": "2024-01-11T20:43:06Z",
        "eventSource": "codeconnections.amazonaws.com",
        "eventName": "CreateHost",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "52.94.133.137",
```

```
        "userAgent": "aws-cli/2.13.30 Python/3.11.6 Darwin/23.2.0 exe/x86_64 prompt/off
 command/codeconnections.create-host",
        "requestParameters": {
            "name": "Demo1",
            "providerType": "GitHubEnterpriseServer",
            "providerEndpoint": "IP"
        },
        "responseElements": {
            "hostArn": "arn:aws:codeconnections:us-east-1:123456789012:host/Demo1-
EXAMPLE"
        },
        "requestID": "974459b3-8a04-4cff-9c8f-0c88647831cc",
        "eventID": "af4ce349-9f21-43fb-8003-267fbf9b1a93",
        "readOnly": false,
        "eventType": "AwsApiCall",
        "managementEvent": true,
        "recipientAccountId": "123456789012",
        "eventCategory": "Management",
        "tlsDetails": {
            "clientProvidedHostHeader": "api.us-east-1.codeconnections.aws.dev"
        }
    }
}
```

`CreateSyncConfiguration` の例

以下の例は、CreateSyncConfiguration アクションを示す CloudTrail ログエントリです。

```
{
    "EventId": "be1397e1-eefb-49f0-b4ee-2708c45e94e7",
    "EventName": "CreateSyncConfiguration",
    "ReadOnly": "false",
    "AccessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "EventTime": "2024-01-24T17:38:30+00:00",
    "EventSource": "codeconnections.amazonaws.com",
    "Username": "Mary_Major",
    "Resources": [],
    "CloudTrailEvent": {
        "eventVersion": "1.08",
        "userIdentity": {
            "type": "AssumedRole",
            "principalId": "AIDACKCEVSQ6C2EXAMPLE",
            "arn": "arn:aws:sts::123456789012:assumed-role/Admin/Mary_Major",
```

```
            "accountId": "123456789012",
            "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
            "sessionContext": {
                "sessionIssuer": {
                    "type": "Role",
                    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                    "arn": "arn:aws:iam::123456789012:role/Admin",
                    "accountId": "123456789012",
                    "userName": "Admin"
                },
                "webIdFederationData": {},
                "attributes": {
                    "creationDate": "2024-01-24T17:34:55Z",
                    "mfaAuthenticated": "false"
                }
            }
        },
        "eventTime": "2024-01-24T17:38:30Z",
        "eventSource": "codeconnections.amazonaws.com",
        "eventName": "CreateSyncConfiguration",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "IP",
        "userAgent": "aws-cli/2.15.11 Python/3.11.6
 Linux/5.10.205-172.804.amzn2int.x86_64exe/x86_64.amzn.2prompt/offcommand/
codeconnections.create-sync-configuration",
        "requestParameters": {
            "branch": "master",
            "configFile": "filename",
            "repositoryLinkId": "6053346f-8a33-4edb-9397-10394b695173",
            "resourceName": "mystack",
            "roleArn": "arn:aws:iam::123456789012:role/my-role",
            "syncType": "CFN_STACK_SYNC"
        },
        "responseElements": {
            "syncConfiguration": {
                "branch": "main",
                "configFile": "filename",
                "ownerId": "owner_ID",
                "providerType": "GitHub",
                "repositoryLinkId": "6053346f-8a33-4edb-9397-10394b695173",
                "repositoryName": "MyGitHubRepo",
                "resourceName": "mystack",
                "roleArn": "arn:aws:iam::123456789012:role/my-role",
                "syncType": "CFN_STACK_SYNC"
```

```
            }
        },
        "requestID": "bad2f662-3f2a-42c0-b638-6115384896f6",
        "eventID": "be1397e1-eefb-49f0-b4ee-2708c45e94e7",
        "readOnly": false,
        "eventType": "AwsApiCall",
        "managementEvent": true,
        "recipientAccountId": "123456789012",
        "eventCategory": "Management",
        "tlsDetails": {
            "clientProvidedHostHeader": "api.us-east-1.codeconnections.aws.dev"
        }
    }
}
```

DeleteConnection の例

以下の例は、DeleteConnection アクションを示す CloudTrail ログエントリです。

```
{
    "EventId": "672837cd-f977-4fe2-95c7-14280b2af76c",
    "EventName": "DeleteConnection",
    "ReadOnly": "false",
    "AccessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "EventTime": "2024-01-10T13:00:50-08:00",
    "EventSource": "codeconnections.amazonaws.com",
    "Username": "Mary_Major",
    "Resources": [],
    "CloudTrailEvent": {
        "eventVersion": "1.08",
        "userIdentity": {
            "type": "AssumedRole",
            "principalId": "AIDACKCEVSQ6C2EXAMPLE",
            "arn": "arn:aws:sts::123456789012:assumed-role/Admin/Mary_Major",
            "accountId": "123456789012",
            "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
            "sessionContext": {
                "sessionIssuer": {
                    "type": "Role",
                    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                    "arn": "arn:aws:iam::001919387613:role/Admin",
                    "accountId": "123456789012",
                    "userName": "Admin"
```

```
                },
                "webIdFederationData": {},
                "attributes": {
                    "creationDate": "2024-01-10T20:41:16Z",
                    "mfaAuthenticated": "false"
                }
            }
        },
        "eventTime": "2024-01-10T21:00:50Z",
        "eventSource": "codeconnections.amazonaws.com",
        "eventName": "DeleteConnection",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "IP",
        "userAgent": "aws-cli/2.13.30 Python/3.11.6 Darwin/23.2.0 exe/x86_64 prompt/off
 command/codeconnections.delete-connection",
        "requestParameters": {
            "connectionArn": "arn:aws:codeconnections:us-
east-1:123456789012:connection/df03df74-8e05-45cf-b420-b39e389dd264"
        },
        "responseElements": null,
        "requestID": "4f26ceab-d665-41df-9e15-5ed0fbb4eca6",
        "eventID": "672837cd-f977-4fe2-95c7-14280b2af76c",
        "readOnly": false,
        "eventType": "AwsApiCall",
        "managementEvent": true,
        "recipientAccountId": "123456789012",
        "eventCategory": "Management",
        "tlsDetails": {
            "clientProvidedHostHeader": "api.us-east-1.codeconnections.aws.dev"
        }
    }
}
```

DeleteHost の例

以下の例は、DeleteHost アクションを示す CloudTrail ログエントリです。

```
{
    "EventId": "6018ba5c-6f24-4a30-b201-16ec19a1687a",
    "EventName": "DeleteHost",
    "ReadOnly": "false",
    "AccessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "EventTime": "2024-01-11T12:56:47-08:00",
```

```
    "EventSource": "codeconnections.amazonaws.com",
    "Username": "Mary_Major",
    "Resources": [],
    "CloudTrailEvent": {
        "eventVersion": "1.08",
        "userIdentity": {
            "type": "AssumedRole",
            "principalId": "AIDACKCEVSQ6C2EXAMPLE",
            "arn": "arn:aws:sts::123456789012:assumed-role/Admin/Mary_Major",
            "accountId": "123456789012",
            "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
            "sessionContext": {
                "sessionIssuer": {
                    "type": "Role",
                    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                    "arn": "arn:aws:iam::123456789012:role/Admin",
                    "accountId": "123456789012",
                    "userName": "Admin"
                },
                "webIdFederationData": {},
                "attributes": {
                    "creationDate": "2024-01-11T20:09:35Z",
                    "mfaAuthenticated": "false"
                }
            }
        },
        "eventTime": "2024-01-11T20:56:47Z",
        "eventSource": "codeconnections.amazonaws.com",
        "eventName": "DeleteHost",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "IP",
        "userAgent": "aws-cli/2.13.30 Python/3.11.6 Darwin/23.2.0 exe/x86_64 prompt/off
 command/codeconnections.delete-host",
        "requestParameters": {
            "hostArn": "arn:aws:codeconnections:us-east-1:123456789012:host/Demo1-
EXAMPLE"
        },
        "responseElements": null,
        "requestID": "1b244528-143a-4028-b9a4-9479e342bce5",
        "eventID": "6018ba5c-6f24-4a30-b201-16ec19a1687a",
        "readOnly": false,
        "eventType": "AwsApiCall",
        "managementEvent": true,
        "recipientAccountId": "123456789012",
```

```
        "eventCategory": "Management",
        "tlsDetails": {
            "clientProvidedHostHeader": "api.us-east-1.codeconnections.aws.dev"
        }
    }
}
```

DeleteSyncConfiguration の例

以下の例は、DeleteSyncConfiguration アクションを示す CloudTrail ログエントリです。

```
{
    "EventId": "588660c7-3202-4998-a906-7bb72bcf4438",
    "EventName": "DeleteSyncConfiguration",
    "ReadOnly": "false",
    "AccessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "EventTime": "2024-01-24T17:41:59+00:00",
    "EventSource": "codeconnections.amazonaws.com",
    "Username": "Mary_Major",
    "Resources": [],
    "CloudTrailEvent": {
        "eventVersion": "1.08",
        "userIdentity": {
            "type": "AssumedRole",
            "principalId": "AIDACKCEVSQ6C2EXAMPLE",
            "arn": "arn:aws:sts::123456789012:assumed-role/Admin/Mary_Major",
            "accountId": "123456789012",
            "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
            "sessionContext": {
                "sessionIssuer": {
                    "type": "Role",
                    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                    "arn": "arn:aws:iam::123456789012:role/Admin",
                    "accountId": "123456789012",
                    "userName": "Admin"
                },
                "webIdFederationData": {},
                "attributes": {
                    "creationDate": "2024-01-24T17:34:55Z",
                    "mfaAuthenticated": "false"
                }
            }
        },
```

```
        "eventTime": "2024-01-24T17:41:59Z",
        "eventSource": "codeconnections.amazonaws.com",
        "eventName": "DeleteSyncConfiguration",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "52.94.133.142",
        "userAgent": "aws-
cli/2.15.11Python/3.11.6Linux/5.10.205-172.804.amzn2int.x86_64exe/x86_64.amzn.2prompt/
offcommand/codeconnections.delete-sync-configuration",
        "requestParameters": {
            "syncType": "CFN_STACK_SYNC",
            "resourceName": "mystack"
        },
        "responseElements": null,
        "requestID": "221e0b1c-a50e-4cf0-ab7d-780154e29c94",
        "eventID": "588660c7-3202-4998-a906-7bb72bcf4438",
        "readOnly": false,
        "eventType": "AwsApiCall",
        "managementEvent": true,
        "recipientAccountId": "123456789012",
        "eventCategory": "Management",
        "tlsDetails": {
            "clientProvidedHostHeader": "api.us-east-1.codeconnections.aws.dev"
        }
    }
}
```

GetConnection の例

以下の例は、GetConnection アクションを示す CloudTrail ログエントリです。

```
{
    "EventId": "672837cd-f977-4fe2-95c7-14280b2af76c",
    "EventName": "DeleteConnection",
    "ReadOnly": "false",
    "AccessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "EventTime": "2024-01-10T13:00:50-08:00",
    "EventSource": "codeconnections.amazonaws.com",
    "Username": "Mary_Major",
    "Resources": [],
    "CloudTrailEvent": {
        "eventVersion": "1.08",
        "userIdentity": {
            "type": "AssumedRole",
```

```
            "principalId": "AIDACKCEVSQ6C2EXAMPLE",
            "arn": "arn:aws:sts::123456789012:assumed-role/Admin/Mary_Major",
            "accountId": "123456789012",
            "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
            "sessionContext": {
                "sessionIssuer": {
                    "type": "Role",
                    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                    "arn": "arn:aws:iam::123456789012:role/Admin",
                    "accountId": "123456789012",
                    "userName": "Admin"
                },
                "webIdFederationData": {},
                "attributes": {
                    "creationDate": "2024-01-10T20:41:16Z",
                    "mfaAuthenticated": "false"
                }
            }
        },
        "eventTime": "2024-01-10T21:00:50Z",
        "eventSource": "codeconnections.amazonaws.com",
        "eventName": "DeleteConnection",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "IP",
        "userAgent": "aws-cli/2.13.30 Python/3.11.6 Darwin/23.2.0 exe/x86_64 prompt/off
 command/codeconnections.delete-connection",
        "requestParameters": {
            "connectionArn": "arn:aws:codeconnections:us-
east-1:123456789012:connection/df03df74-8e05-45cf-b420-b39e389dd264"
        },
        "responseElements": null,
        "requestID": "4f26ceab-d665-41df-9e15-5ed0fbb4eca6",
        "eventID": "672837cd-f977-4fe2-95c7-14280b2af76c",
        "readOnly": false,
        "eventType": "AwsApiCall",
        "managementEvent": true,
        "recipientAccountId": "001919387613",
        "eventCategory": "Management",
        "tlsDetails": {
            "clientProvidedHostHeader": "api.us-east-1.codeconnections.aws.dev"
        }
    }
}
```

GetHost の例

以下の例は、GetHost アクションを示す CloudTrail ログエントリです。


```
{
    "EventId": "faa147e7-fe7c-4ab9-a11b-2568a2883c01",
    "EventName": "GetHost",
    "ReadOnly": "true",
    "AccessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "EventTime": "2024-01-11T12:44:34-08:00",
    "EventSource": "codeconnections.amazonaws.com",
    "Username": "Mary_Major",
    "Resources": [],
    "CloudTrailEvent": {
        "eventVersion": "1.08",
        "userIdentity": {
            "type": "AssumedRole",
            "principalId": "AIDACKCEVSQ6C2EXAMPLE",
            "arn": "arn:aws:sts::123456789012:assumed-role/Admin/Mary_Major",
            "accountId": "123456789012",
            "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
            "sessionContext": {
                "sessionIssuer": {
                    "type": "Role",
                    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                    "arn": "arn:aws:iam::123456789012:role/Admin",
                    "accountId": "123456789012",
                    "userName": "Admin"
                },
                "webIdFederationData": {},
                "attributes": {
                    "creationDate": "2024-01-11T20:09:35Z",
                    "mfaAuthenticated": "false"
                }
            }
        },
        "eventTime": "2024-01-11T20:44:34Z",
        "eventSource": "codeconnections.amazonaws.com",
        "eventName": "GetHost",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "52.94.133.137",
        "userAgent": "aws-cli/2.13.30 Python/3.11.6 Darwin/23.2.0 exe/x86_64 prompt/off
 command/codeconnections.get-host",
        "requestParameters": {
```

```
            "hostArn": "arn:aws:codeconnections:us-east-1:123456789012:host/Demo1-
EXAMPLE"
        },
        "responseElements": null,
        "requestID": "0ad61bb6-f88f-4f96-92fe-997f017ec2bb",
        "eventID": "faa147e7-fe7c-4ab9-a11b-2568a2883c01",
        "readOnly": true,
        "eventType": "AwsApiCall",
        "managementEvent": true,
        "recipientAccountId": "123456789012",
        "eventCategory": "Management",
        "tlsDetails": {
            "clientProvidedHostHeader": "api.us-east-1.codeconnections.aws.dev"
        }
    }
}
```

GetRepositoryLink の例

以下の例は、GetRepositoryLink アクションを示す CloudTrail ログエントリです。

```
{
    "EventId": "b46acb67-3612-41c7-8987-adb6c9ed4ad4",
    "EventName": "GetRepositoryLink",
    "ReadOnly": "false",
    "AccessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "EventTime": "2024-01-24T02:59:28+00:00",
    "EventSource": "codeconnections.amazonaws.com",
    "Username": "Mary_Major",
    "Resources": [],
    "CloudTrailEvent": {
        "eventVersion": "1.08",
        "userIdentity": {
            "type": "AssumedRole",
            "principalId": "AIDACKCEVSQ6C2EXAMPLE",
            "arn": "arn:aws:sts::123456789012:assumed-role/Admin/Mary_Major",
            "accountId": "123456789012",
            "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
            "sessionContext": {
                "sessionIssuer": {
                    "type": "Role",
                    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                    "arn": "arn:aws:iam::123456789012:role/Admin",
```

```
                    "accountId": "123456789012",
                    "userName": "Admin"
                },
                "webIdFederationData": {},
                "attributes": {
                    "creationDate": "2024-01-24T02:58:52Z",
                    "mfaAuthenticated": "false"
                }
            }
        },
        "eventTime": "2024-01-24T02:59:28Z",
        "eventSource": "codeconnections.amazonaws.com",
        "eventName": "GetRepositoryLink",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "IP",
        "userAgent": "aws-cli/2.15.11
 Python/3.11.6Linux/5.10.205-172.804.amzn2int.x86_64 exe/x86_64.amzn.2 prompt/off
 command/codeconnections.get-repository-link",
        "requestParameters": {
            "repositoryLinkId": "6053346f-8a33-4edb-9397-10394b695173"
        },
        "responseElements": {
            "repositoryLinkInfo": {
                "connectionArn": "arn:aws:codeconnections:us-
east-1:123456789012:connection/7df263cc-f055-4843-adef-4ceaefcb2167",
                "ownerId": "123456789012",
                "providerType": "GitHub",
                "repositoryLinkArn": "arn:aws:codeconnections:us-
east-1:123456789012:repository-link/6053346f-8a33-4edb-9397-10394b695173",
                "repositoryLinkId": "6053346f-8a33-4edb-9397-10394b695173",
                "repositoryName": "MyGitHubRepo"
            }
        },
        "requestID": "d46704dd-dbe9-462f-96a6-022a8d319fd1",
        "eventID": "b46acb67-3612-41c7-8987-adb6c9ed4ad4",
        "readOnly": false,
        "eventType": "AwsApiCall",
        "managementEvent": true,
        "recipientAccountId": "123456789012",
        "eventCategory": "Management",
        "tlsDetails": {
            "clientProvidedHostHeader": "api.us-ea-1.codeconnections.aws.dev"
        }
    }
```

```
}
```

GetRepositorySyncStatus の例

次の例は、GetRepositorySyncStatus アクションを示す CloudTrail ログエントリを示しています。

```
{
    "EventId": "3e183b74-d8c4-4ad3-9de3-6b5721c522e9",
    "EventName": "GetRepositorySyncStatus",
    "ReadOnly": "false",
    "AccessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "EventTime": "2024-01-25T03:41:44+00:00",
    "EventSource": "codeconnections.amazonaws.com",
    "Username": "Mary_Major",
    "Resources": [],
    "CloudTrailEvent": {
        "eventVersion": "1.08",
        "userIdentity": {
            "type": "AssumedRole",
            "principalId": "AIDACKCEVSQ6C2EXAMPLE",
            "arn": "arn:aws:sts::123456789012:assumed-role/Admin/Mary_Major",
            "accountId": "123456789012",
            "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
            "sessionContext": {
                "sessionIssuer": {
                    "type": "Role",
                    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                    "arn": "arn:aws:iam::123456789012:role/Admin",
                    "accountId": "123456789012",
                    "userName": "Admin"
                },
                "webIdFederationData": {},
                "attributes": {
                    "creationDate": "2024-01-25T02:56:55Z",
                    "mfaAuthenticated": "false"
                }
            }
        },
        "eventTime": "2024-01-25T03:41:44Z",
        "eventSource": "codeconnections.amazonaws.com",
        "eventName": "GetRepositorySyncStatus",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "52.94.133.138",
```

```
        "userAgent": "aws-cli/2.15.11 Python/3.11.6
 Linux/5.10.205-172.807.amzn2int.x86_64 exe/x86_64.amzn.2 prompt/off command/
codeconnections.get-repository-sync-status",
        "errorCode": "ResourceNotFoundException",
        "errorMessage": "Could not find a sync status for repository
 link:6053346f-8a33-4edb-9397-10394b695173",
        "requestParameters": {
            "branch": "feature-branch",
            "repositoryLinkId": "6053346f-8a33-4edb-9397-10394b695173",
            "syncType": "CFN_STACK_SYNC"
        },
        "responseElements": null,
        "requestID": "e0cee3ee-31e8-4ef5-b749-96cdcabbe36f",
        "eventID": "3e183b74-d8c4-4ad3-9de3-6b5721c522e9",
        "readOnly": false,
        "eventType": "AwsApiCall",
        "managementEvent": true,
        "recipientAccountId": "123456789012",
        "eventCategory": "Management",
        "tlsDetails": {
            "clientProvidedHostHeader": "api.us-east-1.codeconnections.aws.dev"
        }
    }
}
```

GetResourceSyncStatus の例

次の例は、GetResourceSyncStatus アクションを示す CloudTrail ログエントリを示しています。

```
{
    "EventId": "9c47054e-f6f6-4345-96d0-9a5af3954a8d",
    "EventName": "GetResourceSyncStatus",
    "ReadOnly": "false",
    "AccessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "EventTime": "2024-01-25T03:44:11+00:00",
    "EventSource": "codeconnections.amazonaws.com",
    "Username": "Mary_Major",
    "Resources": [],
    "CloudTrailEvent": {
        "eventVersion": "1.08",
        "userIdentity": {
            "type": "AssumedRole",
            "principalId": "AIDACKCEVSQ6C2EXAMPLE",
```

```
            "arn": "arn:aws:sts::123456789012:assumed-role/Admin/Mary_Major",
            "accountId": "123456789012",
            "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
            "sessionContext": {
                "sessionIssuer": {
                    "type": "Role",
                    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                    "arn": "arn:aws:iam::123456789012:role/Admin",
                    "accountId": "123456789012",
                    "userName": "Admin"
                },
                "webIdFederationData": {},
                "attributes": {
                    "creationDate": "2024-01-25T02:56:55Z",
                    "mfaAuthenticated": "false"
                }
            }
        },
        "eventTime": "2024-01-25T03:44:11Z",
        "eventSource": "codeconnections.amazonaws.com",
        "eventName": "GetResourceSyncStatus",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "IP",
        "userAgent": "aws-cli/2.15.11 Python/3.11.6
 Linux/5.10.205-172.807.amzn2int.x86_64 exe/x86_64.amzn.2 prompt/off command/
codeconnections.get-resource-sync-status",
        "requestParameters": {
            "resourceName": "mystack",
            "syncType": "CFN_STACK_SYNC"
        },
        "responseElements": null,
        "requestID": "e74b5503-d651-4920-9fd2-0f40fb5681e0",
        "eventID": "9c47054e-f6f6-4345-96d0-9a5af3954a8d",
        "readOnly": false,
        "eventType": "AwsApiCall",
        "managementEvent": true,
        "recipientAccountId": "123456789012",
        "eventCategory": "Management",
        "tlsDetails": {
            "clientProvidedHostHeader": "api.us-east-1.codeconnections.aws.dev"
        }
    }
}
```

GetSyncBlockerSummary の例

次の例は、GetSyncBlockerSummary アクションを示す CloudTrail ログエントリを示しています。


```
{
    "EventId": "c16699ba-a788-476d-8c6c-47511d76309e",
    "EventName": "GetSyncBlockerSummary",
    "ReadOnly": "false",
    "AccessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "EventTime": "2024-01-25T03:03:02+00:00",
    "EventSource": "codeconnections.amazonaws.com",
    "Username": "Mary_Major",
    "Resources": [],
    "CloudTrailEvent": {
        "eventVersion": "1.08",
        "userIdentity": {
            "type": "AssumedRole",
            "principalId": "AIDACKCEVSQ6C2EXAMPLE",
            "arn": "arn:aws:sts::123456789012:assumed-role/Admin/Mary_Major",
            "accountId": "123456789012",
            "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
            "sessionContext": {
                "sessionIssuer": {
                    "type": "Role",
                    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                    "arn": "arn:aws:iam::123456789012:role/Admin",
                    "accountId": "123456789012",
                    "userName": "Admin"
                },
                "webIdFederationData": {},
                "attributes": {
                    "creationDate": "2024-01-25T02:56:55Z",
                    "mfaAuthenticated": "false"
                }
            }
        },
        "eventTime": "2024-01-25T03:03:02Z",
        "eventSource": "codeconnections.amazonaws.com",
        "eventName": "GetSyncBlockerSummary",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "IP",
        "userAgent": "aws-cli/2.15.11 Python/3.11.6
 Linux/5.10.205-172.807.amzn2int.x86_64 exe/x86_64.amzn.2 prompt/off command/
codeconnections.get-sync-blocker-summary",
```

```
        "requestParameters": {
            "syncType": "CFN_STACK_SYNC",
            "resourceName": "mystack"
        },
        "responseElements": {
            "syncBlockerSummary": {
                "resourceName": "mystack",
                "latestBlockers": []
            }
        },
        "requestID": "04240091-eb25-4138-840d-776f8e5375b4",
        "eventID": "c16699ba-a788-476d-8c6c-47511d76309e",
        "readOnly": false,
        "eventType": "AwsApiCall",
        "managementEvent": true,
        "recipientAccountId": "123456789012",
        "eventCategory": "Management",
        "tlsDetails": {
            "clientProvidedHostHeader": "api.us-east-1.codeconnections.aws.dev"
        }
    }
}
```

GetSyncConfiguration の例

次の例は、GetSyncConfiguration アクションを示す CloudTrail ログエントリを示しています。

```
{
    "EventId": "bab9aa16-4553-4206-a1ea-88219233dd25",
    "EventName": "GetSyncConfiguration",
    "ReadOnly": "false",
    "AccessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "EventTime": "2024-01-24T17:40:40+00:00",
    "EventSource": "codeconnections.amazonaws.com",
    "Username": "Mary_Major",
    "Resources": [],
    "CloudTrailEvent": {
        "eventVersion": "1.08",
        "userIdentity": {
            "type": "AssumedRole",
            "principalId": "AIDACKCEVSQ6C2EXAMPLE",
            "arn": "arn:aws:sts::123456789012:assumed-role/Admin/Mary_Major",
            "accountId": "123456789012",
```

```
            "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
            "sessionContext": {
                "sessionIssuer": {
                    "type": "Role",
                    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                    "arn": "arn:aws:iam::123456789012:role/Admin",
                    "accountId": "123456789012",
                    "userName": "Admin"
                },
                "webIdFederationData": {},
                "attributes": {
                    "creationDate": "2024-01-24T17:34:55Z",
                    "mfaAuthenticated": "false"
                }
            }
        },
        "eventTime": "2024-01-24T17:40:40Z",
        "eventSource": "codeconnections.amazonaws.com",
        "eventName": "GetSyncConfiguration",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "52.94.133.142",
        "userAgent": "aws-
cli/2.15.11Python/3.11.6Linux/5.10.205-172.804.amzn2int.x86_64exe/x86_64.amzn.2prompt/
offcommand/codeconnections.get-sync-configuration",
        "requestParameters": {
            "syncType": "CFN_STACK_SYNC",
            "resourceName": "mystack"
        },
        "responseElements": {
            "syncConfiguration": {
                "branch": "main",
                "configFile": "filename",
                "ownerId": "123456789012",
                "providerType": "GitHub",
                "repositoryLinkId": "6053346f-8a33-4edb-9397-10394b695173",
                "repositoryName": "MyGitHubRepo",
                "resourceName": "mystack",
                "roleArn": "arn:aws:iam::123456789012:role/my-role",
                "syncType": "CFN_STACK_SYNC"
            }
        },
        "requestID": "0aa8e43a-6e34-4d8f-89fb-5c2d01964b35",
        "eventID": "bab9aa16-4553-4206-a1ea-88219233dd25",
        "readOnly": false,
```

```
        "eventType": "AwsApiCall",
        "managementEvent": true,
        "recipientAccountId": "123456789012",
        "eventCategory": "Management",
        "tlsDetails": {
            "clientProvidedHostHeader": "api.us-east-1.codeconnections.aws.dev"
        }
    }
}
```

ListConnections の例

次の例は、ListConnections アクションを示す CloudTrail ログエントリを示しています。

```
{
    "EventId": "3f8d80fe-fbe1-4755-903c-4f58fc8262fa",
    "EventName": "ListConnections",
    "ReadOnly": "true",
    "AccessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "EventTime": "2024-01-08T14:11:23-08:00",
    "EventSource": "codeconnections.amazonaws.com",
    "Username": "Mary_Major",
    "Resources": [],
    "CloudTrailEvent": {
        "eventVersion": "1.08",
        "userIdentity": {
            "type": "AssumedRole",
            "principalId": "AIDACKCEVSQ6C2EXAMPLE",
            "arn": "arn:aws:sts::123456789012:assumed-role/Admin/Mary_Major",
            "accountId": "123456789012",
            "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
            "sessionContext": {
                "sessionIssuer": {
                    "type": "Role",
                    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                    "arn": "arn:aws:iam::123456789012:role/Admin",
                    "accountId": "123456789012",
                    "userName": "Admin"
                },
                "webIdFederationData": {},
                "attributes": {
                    "creationDate": "2024-01-08T22:11:02Z",
                    "mfaAuthenticated": "false"
```

```
                }
            }
        },
        "eventTime": "2024-01-08T22:11:23Z",
        "eventSource": "codeconnections.amazonaws.com",
        "eventName": "ListConnections",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "IP",
        "userAgent": "aws-cli/1.18.147 Python/2.7.18
 Linux/5.10.201-168.748.amzn2int.x86_64 botocore/1.18.6",
        "requestParameters": {
            "maxResults": 50
        },
        "responseElements": null,
        "requestID": "5d456d59-3e92-44be-b941-a429df59e90b",
        "eventID": "3f8d80fe-fbe1-4755-903c-4f58fc8262fa",
        "readOnly": true,
        "eventType": "AwsApiCall",
        "managementEvent": true,
        "recipientAccountId": "123456789012",
        "eventCategory": "Management",
        "tlsDetails": {
            "clientProvidedHostHeader": "api.us-east-1.codeconnections.aws.dev"
        }
    }
}
```

`ListHosts` の例

次の例は、ListHosts アクションを示す CloudTrail ログエントリを示しています。

```
{
    "EventId": "f6e9e831-feaf-4ad1-ac47-51681109c401",
    "EventName": "ListHosts",
    "ReadOnly": "true",
    "AccessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "EventTime": "2024-01-11T13:00:55-08:00",
    "EventSource": "codeconnections.amazonaws.com",
    "Username": "Mary_Major",
    "Resources": [],
    "CloudTrailEvent": {
        "eventVersion": "1.08",
        "userIdentity": {
```

```
            "type": "AssumedRole",
            "principalId": "AIDACKCEVSQ6C2EXAMPLE",
            "arn": "arn:aws:sts::123456789012:assumed-role/Admin/Mary_Major",
            "accountId": "123456789012",
            "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
            "sessionContext": {
                "sessionIssuer": {
                    "type": "Role",
                    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                    "arn": "arn:aws:iam::123456789012:role/Admin",
                    "accountId": "123456789012",
                    "userName": "Admin"
                },
                "webIdFederationData": {},
                "attributes": {
                    "creationDate": "2024-01-11T20:09:35Z",
                    "mfaAuthenticated": "false"
                }
            }
        },
        "eventTime": "2024-01-11T21:00:55Z",
        "eventSource": "codeconnections.amazonaws.com",
        "eventName": "ListHosts",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "IP",
        "userAgent": "aws-cli/2.13.30 Python/3.11.6 Darwin/23.2.0 exe/x86_64 prompt/off
 command/codeconnections.list-hosts",
        "requestParameters": {
            "maxResults": 50
        },
        "responseElements": null,
        "requestID": "ea87e2cf-6bf1-4cc7-9666-f3fad85d6d83",
        "eventID": "f6e9e831-feaf-4ad1-ac47-51681109c401",
        "readOnly": true,
        "eventType": "AwsApiCall",
        "managementEvent": true,
        "recipientAccountId": "123456789012",
        "eventCategory": "Management",
        "tlsDetails": {
            "clientProvidedHostHeader": "api.us-east-1.codeconnections.aws.dev"
        }
    }
}
```

ListRepositoryLinks の例

次の例は、ListRepositoryLinks アクションを示す CloudTrail ログエントリを示しています。


```
{
    "EventId": "4f714bbb-0716-4f6e-9868-9b379b30757f",
    "EventName": "ListRepositoryLinks",
    "ReadOnly": "false",
    "AccessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "EventTime": "2024-01-24T01:57:29+00:00",
    "EventSource": "codeconnections.amazonaws.com",
    "Username": "Mary_Major",
    "Resources": [],
    "CloudTrailEvent": {
        "eventVersion": "1.08",
        "userIdentity": {
            "type": "AssumedRole",
            "principalId": "AIDACKCEVSQ6C2EXAMPLE",
            "arn": "arn:aws:sts::123456789012:assumed-role/Admin/Mary_Major",
            "accountId": "123456789012",
            "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
            "sessionContext": {
                "sessionIssuer": {
                    "type": "Role",
                    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                    "arn": "arn:aws:iam::123456789012:role/Admin",
                    "accountId": "123456789012",
                    "userName": "Admin"
                },
                "webIdFederationData": {},
                "attributes": {
                    "creationDate": "2024-01-24T01:43:49Z",
                    "mfaAuthenticated": "false"
                }
            }
        },
        "eventTime": "2024-01-24T01:57:29Z",
        "eventSource": "codeconnections.amazonaws.com",
        "eventName": "ListRepositoryLinks",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "IP",
        "userAgent": "aws-
cli/2.15.11Python/3.11.6Linux/5.10.205-172.804.amzn2int.x86_64exe/x86_64.amzn.2prompt/
offcommand/codeconnections.list-repository-links",
```

```
        "requestParameters": {
            "maxResults": 50
        },
        "responseElements": {
            "repositoryLinks": [
                {
                    "connectionArn": "arn:aws:codeconnections:us-
east-1:123456789012:connection/001f5be2-a661-46a4-b96b-4d277cac8b6e",
                    "ownerId": "123456789012",
                    "providerType": "GitHub",
                    "repositoryLinkArn": "arn:aws:codeconnections:us-
east-1:123456789012:repository-link/be8f2017-b016-4a77-87b4-608054f70e77",
                    "repositoryLinkId": "be8f2017-b016-4a77-87b4-608054f70e77",
                    "repositoryName": "MyGitHubRepo"
                },
                {
                    "connectionArn": "arn:aws:codeconnections:us-
east-1:123456789012:connection/7df263cc-f055-4843-adef-4ceaefcb2167",
                    "ownerId": "owner",
                    "providerType": "GitHub",
                    "repositoryLinkArn": "arn:aws:codeconnections:us-
east-1:123456789012:repository-link/6053346f-8a33-4edb-9397-10394b695173",
                    "repositoryLinkId": "6053346f-8a33-4edb-9397-10394b695173",
                    "repositoryName": "MyGitHubRepo"
                }
            ]
        },
        "requestID": "7c8967a9-ec15-42e9-876b-0ef58681ec55",
        "eventID": "4f714bbb-0716-4f6e-9868-9b379b30757f",
        "readOnly": false,
        "eventType": "AwsApiCall",
        "managementEvent": true,
        "recipientAccountId": "123456789012",
        "eventCategory": "Management",
        "tlsDetails": {
            "clientProvidedHostHeader": "api.us-east-1.codeconnections.aws.dev"
        }
    }
}
```

ListRepositorySyncDefinitions の例

次の例は、ListRepositorySyncDefinitions アクションを示す CloudTrail ログエントリを示しています。


```
{
    "EventId": "12e52dbb-b00d-49ad-875a-3efec36e5aa1",
    "EventName": "ListRepositorySyncDefinitions",
    "ReadOnly": "false",
    "AccessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "EventTime": "2024-01-25T16:56:19+00:00",
    "EventSource": "codeconnections.amazonaws.com",
    "Username": "Mary_Major",
    "Resources": [],
    "CloudTrailEvent": {
        "eventVersion": "1.08",
        "userIdentity": {
            "type": "AssumedRole",
            "principalId": "AIDACKCEVSQ6C2EXAMPLE",
            "arn": "arn:aws:sts::123456789012:assumed-role/Admin/Mary_Major",
            "accountId": "123456789012",
            "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
            "sessionContext": {
                "sessionIssuer": {
                    "type": "Role",
                    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                    "arn": "arn:aws:iam::123456789012:role/Admin",
                    "accountId": "123456789012",
                    "userName": "Admin"
                },
                "webIdFederationData": {},
                "attributes": {
                    "creationDate": "2024-01-25T16:43:03Z",
                    "mfaAuthenticated": "false"
                }
            }
        },
        "eventTime": "2024-01-25T16:56:19Z",
        "eventSource": "codeconnections.amazonaws.com",
        "eventName": "ListRepositorySyncDefinitions",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "IP",
```

```
        "userAgent": "aws-cli/2.15.11 Python/3.11.6
 Linux/5.10.205-172.807.amzn2int.x86_64 exe/x86_64.amzn.2 prompt/off command/
codeconnections.list-repository-sync-definitions",
        "requestParameters": {
            "repositoryLinkId": "6053346f-8a33-4edb-9397-10394b695173",
            "syncType": "CFN_STACK_SYNC",
            "maxResults": 50
        },
        "responseElements": {
            "repositorySyncDefinitions": []
        },
        "requestID": "df31d11d-5dc7-459b-9a8f-396b4769cdd9",
        "eventID": "12e52dbb-b00d-49ad-875a-3efec36e5aa1",
        "readOnly": false,
        "eventType": "AwsApiCall",
        "managementEvent": true,
        "recipientAccountId": "123456789012",
        "eventCategory": "Management",
        "tlsDetails": {
            "clientProvidedHostHeader": "api.us-east-1.codeconnections.aws.dev"
        }
    }
```


`ListSyncConfigurations` の例

次の例は、ListSyncConfigurations アクションを示す CloudTrail ログエントリを示しています。


```
{
    "EventId": "aa4ae557-ec31-4151-8d21-9e74dd01344c",
    "EventName": "ListSyncConfigurations",
    "ReadOnly": "false",
    "AccessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "EventTime": "2024-01-24T17:42:06+00:00",
    "EventSource": "codeconnections.amazonaws.com",
    "Username": "Mary_Major",
    "Resources": [],
    "CloudTrailEvent": {
        "eventVersion": "1.08",
        "userIdentity": {
            "type": "AssumedRole",
            "type": "AssumedRole",
            "principalId": "AIDACKCEVSQ6C2EXAMPLE",
            "arn": "arn:aws:sts::123456789012:assumed-role/Admin/Mary_Major",
```

```
            "accountId": "123456789012",
            "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
            "sessionContext": {
                "sessionIssuer": {
                    "type": "Role",
                    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                    "arn": "arn:aws:iam::123456789012:role/Admin",
                    "accountId": "123456789012",
                    "userName": "Admin"
                },
                "webIdFederationData": {},
                "attributes": {
                    "creationDate": "2024-01-24T17:34:55Z",
                    "mfaAuthenticated": "false"
                }
            }
        },
        "eventTime": "2024-01-24T17:42:06Z",
        "eventSource": "codeconnections.amazonaws.com",
        "eventName": "ListSyncConfigurations",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "IP",
        "userAgent": "aws-cli/2.15.11 Python/3.11.6
 Linux/5.10.205-172.804.amzn2int.x86_64 exe/x86_64.amzn.2 prompt/offcommand/
codeconnections.list-sync-configurations",
        "requestParameters": {
            "maxResults": 50,
            "repositoryLinkId": "6053346f-8a33-4edb-9397-10394b695173",
            "syncType": "CFN_STACK_SYNC"
        },
        "responseElements": {
            "syncConfigurations": [
                {
                    "branch": "feature-branch",
                    "configFile": "filename.yaml",
                    "ownerId": "owner",
                    "providerType": "GitHub",
                    "repositoryLinkId": "6053346f-8a33-4edb-9397-10394b695173",
                    "repositoryName": "MyGitHubRepo",
                    "resourceName": "dkstacksync",
                    "roleArn": "arn:aws:iam::123456789012:role/my-role",
                    "syncType": "CFN_STACK_SYNC"
                }
            ]
```

```
        },
        "requestID": "7dd220b5-fc0f-4023-aaa0-9555cfe759df",
        "eventID": "aa4ae557-ec31-4151-8d21-9e74dd01344c",
        "readOnly": false,
        "eventType": "AwsApiCall",
        "managementEvent": true,
        "recipientAccountId": "123456789012",
        "eventCategory": "Management",
        "tlsDetails": {
            "clientProvidedHostHeader": "api.us-east-1.codeconnections.aws.dev"
        }
    }
}
```

`ListTagsForResource` の例

次の例は、ListTagsForResource アクションを示す CloudTrail ログエントリを示しています。

```
{
    "EventId": "fc501054-d68a-4325-824c-0e34062ef040",
    "EventName": "ListTagsForResource",
    "ReadOnly": "true",
    "AccessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "EventTime": "2024-01-25T17:16:56+00:00",
    "EventSource": "codeconnections.amazonaws.com",
    "Username": "dMary_Major",
    "Resources": [],
    "CloudTrailEvent": {
        "eventVersion": "1.08",
        "userIdentity": {
            "type": "AssumedRole",
            "principalId": "AIDACKCEVSQ6C2EXAMPLE",
            "arn": "arn:aws:sts::123456789012:assumed-role/Admin/Mary_Major",
            "accountId": "123456789012",
            "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
            "sessionContext": {
                "sessionIssuer": {
                    "type": "Role",
                    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                    "arn": "arn:aws:iam::123456789012:role/Admin",
                    "accountId": "123456789012",
                    "userName": "Admin"
                },
```

```
                "webIdFederationData": {},
                "attributes": {
                    "creationDate": "2024-01-25T16:43:03Z",
                    "mfaAuthenticated": "false"
                }
            }
        },
        "eventTime": "2024-01-25T17:16:56Z",
        "eventSource": "codeconnections.amazonaws.com",
        "eventName": "ListTagsForResource",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "IP",
        "userAgent": "aws-cli/2.15.11 Python/3.11.6
 Linux/5.10.205-172.807.amzn2int.x86_64 exe/x86_64.amzn.2 prompt/off command/
codeconnections.list-tags-for-resource",
        "requestParameters": {
            "resourceArn": "arn:aws:codeconnections:us-
east-1:123456789012:connection/9703702f-bebe-41b7-8fc4-8e6d2430a330"
        },
        "responseElements": null,
        "requestID": "994584a3-4807-47f2-bb1b-a64f0af6c250",
        "eventID": "fc501054-d68a-4325-824c-0e34062ef040",
        "readOnly": true,
        "eventType": "AwsApiCall",
        "managementEvent": true,
        "recipientAccountId": "123456789012",
        "eventCategory": "Management",
        "tlsDetails": {
            "clientProvidedHostHeader": "api.us-east-1.codeconnections.aws.dev"
        }
    }
}
```

TagResource の例

次の例は、TagResource アクションを示す CloudTrail ログエントリを示しています。

```
{
    "EventId": "b7fbc943-2dd1-4c5b-a5ad-fc6d60a011f1",
    "EventName": "TagResource",
    "ReadOnly": "false",
    "AccessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "EventTime": "2024-01-11T12:22:11-08:00",
```

```
    "EventSource": "codeconnections.amazonaws.com",
    "Username": "Mary_Major",
    "Resources": [],
    "CloudTrailEvent": {
        "eventVersion": "1.08",
        "userIdentity": {
            "type": "AssumedRole",
            "principalId": "AIDACKCEVSQ6C2EXAMPLE",
            "arn": "arn:aws:sts::123456789012:assumed-role/Admin/Mary_Major",
            "accountId": "123456789012",
            "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
            "sessionContext": {
                "sessionIssuer": {
                    "type": "Role",
                    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                    "arn": "arn:aws:iam::123456789012:role/Admin",
                    "accountId": "123456789012",
                    "userName": "Admin"
                },
                "webIdFederationData": {},
                "attributes": {
                    "creationDate": "2024-01-11T20:09:35Z",
                    "mfaAuthenticated": "false"
                }
            }
        },
        "eventTime": "2024-01-11T20:22:11Z",
        "eventSource": "codeconnections.amazonaws.com",
        "eventName": "TagResource",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "IP",
        "userAgent": "aws-cli/2.13.30 Python/3.11.6 Darwin/23.2.0 exe/x86_64 prompt/off
 command/codeconnections.tag-resource",
        "requestParameters": {
            "resourceArn": "arn:aws:codeconnections:us-
east-1:123456789012:connection/8dcf69d1-3316-4392-ae09-71e038adb6ed",
            "tags": [
                {
                    "key": "Demo1",
                    "value": "hhvh1"
                }
            ]
        },
        "responseElements": null,
```

```
        "requestID": "ba382c33-7124-48c8-a23a-25816ce27604",
        "eventID": "b7fbc943-2dd1-4c5b-a5ad-fc6d60a011f1",
        "readOnly": false,
        "eventType": "AwsApiCall",
        "managementEvent": true,
        "recipientAccountId": "123456789012",
        "eventCategory": "Management",
        "tlsDetails": {
            "clientProvidedHostHeader": "api.us-east-1.codeconnections.aws.dev"
        }
    }
}
```

UnTagResource の例

次の例は、UntagResource アクションを示す CloudTrail ログエントリを示しています。

```
{
    "EventId": "8a85cdee-2586-4679-be18-eec34204bc7e",
    "EventName": "UntagResource",
    "ReadOnly": "false",
    "AccessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "EventTime": "2024-01-11T12:31:14-08:00",
    "EventSource": "codeconnections.amazonaws.com",
    "Username": "Mary_Major",
    "Resources": [],
    "CloudTrailEvent": {
        "eventVersion": "1.08",
        "userIdentity": {
            "type": "AssumedRole",
            "principalId": "AIDACKCEVSQ6C2EXAMPLE",
            "arn": "arn:aws:sts::123456789012:assumed-role/Admin/Mary_Major",
            "accountId": "123456789012",
            "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
            "sessionContext": {
                "sessionIssuer": {
                    "type": "Role",
                    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                    "arn": "arn:aws:iam::123456789012:role/Admin",
                    "accountId": "123456789012",
                    "userName": "Admin"
                },
                "webIdFederationData": {},
```

```
                "attributes": {
                    "creationDate": "2024-01-11T20:09:35Z",
                    "mfaAuthenticated": "false"
                }
            }
        },
        "eventTime": "2024-01-11T20:31:14Z",
        "eventSource": "codeconnections.amazonaws.com",
        "eventName": "UntagResource",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "IP",
        "userAgent": "aws-cli/2.13.30 Python/3.11.6 Darwin/23.2.0 exe/x86_64 prompt/off
 command/codeconnections.untag-resource",
        "requestParameters": {
            "resourceArn": "arn:aws:codeconnections:us-
east-1:123456789012:connection/8dcf69d1-3316-4392-ae09-71e038adb6ed",
            "tagKeys": [
                "Project",
                "ReadOnly"
            ]
        },
        "responseElements": null,
        "requestID": "05ef26a4-8c39-4f72-89bf-0c056c51b8d7",
        "eventID": "8a85cdee-2586-4679-be18-eec34204bc7e",
        "readOnly": false,
        "eventType": "AwsApiCall",
        "managementEvent": true,
        "recipientAccountId": "123456789012",
        "eventCategory": "Management",
        "tlsDetails": {
            "clientProvidedHostHeader": "api.us-east-1.codeconnections.aws.dev"
        }
    }
}
```


UpdateHost の例

次の例は、UpdateHost アクションを示す CloudTrail ログエントリを示しています。


```
"Events": [{
        "EventId": "4307cf7d-6d1c-40d9-a659-1bb41b31a2b6",
        "EventName": "UpdateHost",
        "ReadOnly": "false",
```

```
        "AccessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "EventTime": "2024-01-11T12:54:32-08:00",
        "EventSource": "codeconnections.amazonaws.com",
        "Username": "Mary_Major",
        "Resources": [],
        "CloudTrailEvent": "eventVersion": "1.08",
        "userIdentity": {
            "type": "AssumedRole",
            "principalId": "AIDACKCEVSQ6C2EXAMPLE",
            "arn": "arn:aws:sts::123456789012:assumed-role/Admin/Mary_Major",
            "accountId": "123456789012",
            "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
            "sessionContext": {
                "sessionIssuer": {
                    "type": "Role",
                    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                    "arn": "arn:aws:iam::123456789012:role/Admin",
                    "accountId": "123456789012",
                    "userName": "Admin"
                },
                "webIdFederationData": {},
                "attributes": {
                    "creationDate": "2024-01-11T20:09:35Z",
                    "mfaAuthenticated": "false"
                }
            }
        },
        "eventTime": "2024-01-11T20:54:32Z",
        "eventSource": "codeconnections.amazonaws.com",
        "eventName": "UpdateHost",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "IP",
        "userAgent": "aws-cli/2.13.30 Python/3.11.6 Darwin/23.2.0 exe/x86_64 prompt/off
 command/codeconnections.update-host",
        "requestParameters": {
            "hostArn": "arn:aws:codeconnections:us-east-1:123456789012:host/
Demo1-34e70ecb",
            "providerEndpoint": "https://54.218.245.167"
        },
        "responseElements": null,
        "requestID": "b17f46ac-1acb-44ab-a9f5-c35c20233441",
        "eventID": "4307cf7d-6d1c-40d9-a659-1bb41b31a2b6",
        "readOnly": false,
        "eventType": "AwsApiCall",
```

```
        "managementEvent": true,
        "recipientAccountId": "123456789012",
        "eventCategory": "Management",
        "tlsDetails": {
            "clientProvidedHostHeader": "api.us-east-1.codeconnections.aws.dev"
        }
```

UpdateRepositoryLink の例

次の例は、UpdateRepositoryLink アクションを示す CloudTrail ログエントリを示しています。

```
{
    "EventId": "be358c9a-5a8f-467e-8585-2860070be4fe",
    "EventName": "UpdateRepositoryLink",
    "ReadOnly": "false",
    "AccessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "EventTime": "2024-01-24T02:03:24+00:00",
    "EventSource": "codeconnections.amazonaws.com",
    "Username": "Mary_Major",
    "Resources": [],
    "CloudTrailEvent": {
        "eventVersion": "1.08",
        "userIdentity": {
            "type": "AssumedRole",
            "principalId": "AIDACKCEVSQ6C2EXAMPLE",
            "arn": "arn:aws:sts::123456789012:assumed-role/Admin/Mary_Major",
            "accountId": "123456789012",
            "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
            "sessionContext": {
                "sessionIssuer": {
                    "type": "Role",
                    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                    "arn": "arn:aws:iam::123456789012:role/Admin",
                    "accountId": "123456789012",
                    "userName": "Admin"
                },
                "webIdFederationData": {},
                "attributes": {
                    "creationDate": "2024-01-24T01:43:49Z",
                    "mfaAuthenticated": "false"
                }
            }
        },
```

```
        "eventTime": "2024-01-24T02:03:24Z",
        "eventSource": "codeconnections.amazonaws.com",
        "eventName": "UpdateRepositoryLink",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "IP",
        "userAgent": "aws-
cli/2.15.11Python/3.11.6Linux/5.10.205-172.804.amzn2int.x86_64exe/x86_64.amzn.2prompt/
offcommand/codeconnections.update-repository-link",
        "requestParameters": {
            "connectionArn": "arn:aws:codeconnections:us-
east-1:123456789012:connection/7df263cc-f055-4843-adef-4ceaefcb2167",
            "repositoryLinkId": "6053346f-8a33-4edb-9397-10394b695173"
        },
        "responseElements": {
            "repositoryLinkInfo": {
                "connectionArn": "arn:aws:codeconnections:us-
east-1:123456789012:connection/7df263cc-f055-4843-adef-4ceaefcb2167",
                "ownerId": "owner",
                "providerType": "GitHub",
                "repositoryLinkArn": "arn:aws:codeconnections:us-
east-1:123456789012:repository-link/6053346f-8a33-4edb-9397-10394b695173",
                "repositoryLinkId": "6053346f-8a33-4edb-9397-10394b695173",
                "repositoryName": "MyGitHubRepo"
            }
        },
        "additionalEventData": {
            "providerAction": "UpdateRepositoryLink"
        },
        "requestID": "e01eee49-9393-4983-89e4-d1b3353a70d9",
        "eventID": "be358c9a-5a8f-467e-8585-2860070be4fe",
        "readOnly": false,
        "eventType": "AwsApiCall",
        "managementEvent": true,
        "recipientAccountId": "123456789012",
        "eventCategory": "Management",
        "tlsDetails": {
            "clientProvidedHostHeader": "api.us-east-1.codeconnections.aws.dev"
        }
    }
}
```

UpdateSyncBlocker の例

次の例は、UpdateSyncBlocker アクションを示す CloudTrail ログエントリを示しています。


```
{
    "EventId": "211d19db-9f71-4d93-bf90-10f9ddefed88",
    "EventName": "UpdateSyncBlocker",
    "ReadOnly": "false",
    "AccessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "EventTime": "2024-01-25T03:01:05+00:00",
    "EventSource": "codeconnections.amazonaws.com",
    "Username": "Mary_Major",
    "Resources": [],
    "CloudTrailEvent": {
        "eventVersion": "1.08",
        "userIdentity": {
            "type": "AssumedRole",
            "principalId": "AIDACKCEVSQ6C2EXAMPLE",
            "arn": "arn:aws:sts::123456789012:assumed-role/Admin/Mary_Major",
            "accountId": "123456789012",
            "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
            "sessionContext": {
                "sessionIssuer": {
                    "type": "Role",
                    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                    "arn": "arn:aws:iam::123456789012:role/Admin",
                    "accountId": "123456789012",
                    "userName": "Admin"
                },
                "webIdFederationData": {},
                "attributes": {
                    "creationDate": "2024-01-25T02:56:55Z",
                    "mfaAuthenticated": "false"
                }
            }
        },
        "eventTime": "2024-01-25T03:01:05Z",
        "eventSource": "codeconnections.amazonaws.com",
        "eventName": "UpdateSyncBlocker",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "IP",
        "userAgent": "aws-cli/2.15.11 Python/3.11.6
 Linux/5.10.205-172.807.amzn2int.x86_64 exe/x86_64.amzn.2 prompt/off command/
codeconnections.update-sync-blocker",
```

```
        "requestParameters": {
            "id": "ID",
            "syncType": "CFN_STACK_SYNC",
            "resourceName": "mystack",
            "resolvedReason": "Reason"
        },
        "responseElements": null,
        "requestID": "eea03b39-b299-4099-ba55-608480f8d96d",
        "eventID": "211d19db-9f71-4d93-bf90-10f9ddefed88",
        "readOnly": false,
        "eventType": "AwsApiCall",
        "managementEvent": true,
        "recipientAccountId": "123456789012",
        "eventCategory": "Management",
        "tlsDetails": {
            "clientProvidedHostHeader": "api.us-east-1.codeconnections.aws.dev"
        }
    }
}
```

UpdateSyncConfiguration の例

次の例は、UpdateSyncConfiguration アクションを示す CloudTrail ログエントリを示しています。

```
{
    "EventId": "d961c94f-1881-4fe8-83bf-d04cb9f22577",
    "EventName": "UpdateSyncConfiguration",
    "ReadOnly": "false",
    "AccessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "EventTime": "2024-01-24T17:40:55+00:00",
    "EventSource": "codeconnections.amazonaws.com",
    "Username": "Mary_Major",
    "Resources": [],
    "CloudTrailEvent": {
        "eventVersion": "1.08",
        "userIdentity": {
            "type": "AssumedRole",
            "principalId": "AIDACKCEVSQ6C2EXAMPLE",
            "arn": "arn:aws:sts::123456789012:assumed-role/Admin/Mary_Major",
            "accountId": "123456789012",
            "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
            "sessionContext": {
                "sessionIssuer": {
```

```
                    "type": "Role",
                    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                    "arn": "arn:aws:iam::123456789012:role/Admin",
                    "accountId": "123456789012",
                    "userName": "Admin"
                },
                "webIdFederationData": {},
                "attributes": {
                    "creationDate": "2024-01-24T17:34:55Z",
                    "mfaAuthenticated": "false"
                }
            }
        },
        "eventTime": "2024-01-24T17:40:55Z",
        "eventSource": "codeconnections.amazonaws.com",
        "eventName": "UpdateSyncConfiguration",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "IP",
        "userAgent": "aws-cli/2.15.11
 Python/3.11.6Linux/5.10.205-172.804.amzn2int.x86_64exe/x86_64.amzn.2prompt/offcommand/
codeconnections.update-sync-configuration",
        "requestParameters": {
            "branch": "feature-branch",
            "resourceName": "mystack",
            "syncType": "CFN_STACK_SYNC"
        },
        "responseElements": {
            "syncConfiguration": {
                "branch": "feature-branch",
                "configFile": "filename",
                "ownerId": "owner",
                "providerType": "GitHub",
                "repositoryLinkId": "6053346f-8a33-4edb-9397-10394b695173",
                "repositoryName": "MyGitHubRepo",
                "resourceName": "mystack",
                "roleArn": "arn:aws:iam::123456789012:role/my-role",
                "syncType": "CFN_STACK_SYNC"
            }
        },
        "requestID": "2ca545ef-4395-4e1f-b14a-2750481161d6",
        "eventID": "d961c94f-1881-4fe8-83bf-d04cb9f22577",
        "readOnly": false,
        "eventType": "AwsApiCall",
        "managementEvent": true,
```

```
        "recipientAccountId": "123456789012",
        "eventCategory": "Management",
        "tlsDetails": {
            "clientProvidedHostHeader": "api.us-east-1.codeconnections.aws.dev"
        }
    }
}
```

AWS CodeConnections およびインターフェイス VPC エンドポイント (AWS PrivateLink)

VPC と の間にプライベート接続を確立するには、インターフェイス VPC エンドポイント AWS CodeConnections を作成します。インターフェイスエンドポイントは、インターネットゲートウェイAWS PrivateLink、NAT デバイス、VPN 接続、または AWS Direct Connect 接続なしで AWS CodeConnections APIs にプライベートにアクセスできるテクノロジーである を利用しています。VPC 内のインスタンスは、パブリック IP アドレスがなくても AWS CodeConnections APIsと通信できます。VPC と 間のトラフィック AWS CodeConnections は Amazon ネットワークを離れないためです。

各インターフェースエンドポイントは、サブネット内の 1 つ以上の Elastic Network Interface によって表されます。

詳細については、Amazon VPC ユーザーガイドの「インターフェイス VPC エンドポイント (AWS PrivateLink)」を参照してください。

AWS CodeConnections VPC エンドポイントに関する考慮事項

のインターフェイス VPC エンドポイントを設定する前に AWS CodeConnections、「Amazon VPC ユーザーガイド」の「インターフェイスエンドポイント」を確認してください。

AWS CodeConnections は、VPC からのすべての API アクションの呼び出しをサポートしています。

VPC エンドポイントはすべての AWS CodeConnections リージョンでサポートされています。

VPC エンドポイントの概念

VPC エンドポイントの主な概念は次のとおりです。

VPC エンドポイント

サービスへのプライベート接続を可能にする VPC 内のエントリポイント。VPC エンドポイントのさまざまなタイプを次に示します。サポートされるサービスにより要求される VPC エンドポイントのタイプを作成します。

- AWS CodeConnections アクションの VPC エンドポイント
- AWS CodeConnections ウェブフックの VPC エンドポイント

AWS PrivateLink

VPC とサービスの間にプライベート接続を提供するテクノロジー。

AWS CodeConnections アクションの VPC エンドポイント

AWS CodeConnections サービスの VPC エンドポイントを管理できます。

AWS CodeConnections アクションのインターフェイス VPC エンドポイントの作成

Amazon VPC コンソールまたは AWS Command Line Interface () を使用して、 AWS CodeConnections サービスの VPC エンドポイントを作成できますAWS CLI。詳細については、「Amazon VPC ユーザーガイド」のインターフェイスエンドポイントの作成を参照してください。

VPC との接続の使用を開始するには、 のインターフェイス VPC エンドポイントを作成します AWS CodeConnections。の VPC エンドポイントを作成するときに AWS CodeConnections、AWS サービスを選択し、サービス名で以下を選択します。

- com.amazonaws.***region***.codestar-connections.api: このオプションは、 AWS CodeConnections API オペレーション用の VPC エンドポイントを作成します。たとえば、ユーザーが CLI、 AWS CodeConnections API、または AWS SDKs AWS を使用して `CreateConnection`、、 などのオペレーション AWS CodeConnections で を操作する場合は`ListConnections`、このオプションを選択します`CreateHost`。

DNS 名を有効にするオプションでは、エンドポイントにプライベート DNS を選択した場合、 などのリージョンのデフォルト DNS 名 AWS CodeConnections を使用して に API リクエストを行うことができます`codestar-connections.us-east-1.amazonaws.com`。

> **Important**
>
> プライベート DNS は、 AWS サービスおよび AWS Marketplace パートナーサービス用に作成されたエンドポイントに対してデフォルトで有効になっています。

詳細については、「Amazon VPC ユーザーガイド」の「インターフェイスエンドポイントを介したサービスへのアクセス」を参照してください。

AWS CodeConnections アクションの VPC エンドポイントポリシーの作成

VPC エンドポイントには、 AWS CodeConnectionsへのアクセスを制御するエンドポイントポリシーをアタッチできます。このポリシーでは、以下の情報を指定します。

- アクションを実行できるプリンシパル。
- 実行可能なアクション。
- アクションを実行できるリソース。

詳細については、「Amazon VPC ユーザーガイド」の「VPC エンドポイントでサービスへのアクセスを制御する」を参照してください。

> **Note**
>
> com.amazonaws.*region*.codestar-connections.webhooks エンドポイントは、ポリシーをサポートしていません。

例: AWS CodeConnections アクションの VPC エンドポイントポリシー

以下は、 のエンドポイントポリシーの例です AWS CodeConnections。エンドポイントにアタッチすると、このポリシーは、すべてのリソースのすべてのプリンシパルに対して、リストされた AWS CodeConnections アクションへのアクセスを許可します。

```
{
  "Statement": [
    {
      "Sid": "GetConnectionOnly",
      "Principal": "*",
```

```
      "Action": [
        "codestar-connections:GetConnection"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

AWS CodeConnections ウェブフックの VPC エンドポイント

AWS CodeConnections は、VPC 設定でホストを作成または削除するときに、ウェブフックエンドポイントを作成します。エンドポイント名は com.amazonaws.***region***.codestar-connections.webhooks です。

GitHub ウェブフックの VPC エンドポイントを使用すると、ホストはウェブフックを介してイベントデータを Amazon ネットワーク経由で統合 AWS サービスに送信できます。

> **Important**
>
> GitHub Enterprise Server のホストを設定すると、 はウェブフックイベントデータ用の VPC エンドポイント AWS CodeConnections を作成します。2020 年 11 月 24 日より前にホストを作成し、VPC PrivateLink ウェブフックエンドポイントを使用する場合は、最初にホストを削除してから、新しいホストを作成する必要があります。

AWS CodeConnections は、これらのエンドポイントのライフサイクルを管理します。エンドポイントを削除するには、対応するホストリソースを削除する必要があります。

AWS CodeConnections ホストのウェブフックエンドポイントの使用方法

ウェブフックエンドポイントは、サードパーティーリポジトリからのウェブフックが AWS CodeConnections 処理のために送信される場所です。ウェブフックでは、顧客のアクションを説明します。`git push` を実行すると、ウェブフックエンドポイントはプロバイダーからプッシュの詳細を示すウェブフックを受信します。たとえば、 AWS CodeConnections は CodePipeline に通知してパイプラインを開始できます。

Bitbucket などのクラウドプロバイダーや VPC を使用しない GitHub Enterprise Server ホストの場合、プロバイダーは Amazon ネットワークが使用されていない AWS CodeConnections 場所にウェブフックを送信しているため、ウェブフック VPC エンドポイントは適用されません。

接続のトラブルシューティング

以下の情報は、、、 AWS CodeBuild AWS CodeDeployおよび のリソースへの接続に関する一般的な問題のトラブルシューティングに役立ちます AWS CodePipeline。

トピック

接続を作成できません

接続を作成するためのアクセス許可がない可能性があります。詳細については、「のアクセス許可と例 AWS CodeConnections」を参照してください。

接続を作成または完了しようとすると、アクセス許可エラーが表示される

CodePipeline コンソールで接続を作成または表示しようとすると、次のエラーメッセージが返されることがあります。

User: *username* is not authorized to perform: *permission* on resource: *connection-ARN*

このメッセージが表示された場合は、アクセス許可が十分であることを確認してください。

AWS Command Line Interface (AWS CLI) または AWS マネジメントコンソール で接続を作成および表示するアクセス許可は、コンソールで接続を作成および完了するために必要なアクセス許可の一部にすぎません。単に接続を表示、編集、または作成してから保留中の接続を完了するために必要なアクセス許可は、特定のタスクだけを実行する必要があるユーザーを対象に絞り込む必要があります。詳細については、「のアクセス許可と例 AWS CodeConnections」を参照してください。

接続を使用しようとすると、アクセス許可エラーが表示されます

CodePipeline コンソールで接続を使用しようとすると、アクセス許可の一覧表示、取得、および作成のアクセス許可がある場合でも、次のエラーメッセージのいずれかまたは両方が返されることがあります。

You have failed to authenticate your account.(アカウントの認証に失敗しました。)

User: *username* is not authorized to perform: codestar-connections:UseConnection on resource: *connection-ARN*

これが発生した場合、アクセス許可が十分であることを確認してください。

プロバイダーの場所で使用可能なリポジトリーをリストするなど、接続を使用するためのアクセス許可があることを確認してください。 詳細については、「のアクセス許可と例 AWS CodeConnections」を参照してください。

接続が使用可能な状態でないか、または保留中ではなくなりました

接続が使用可能な状態ではないというメッセージがコンソールに表示される場合は、[Complete connection] (完全な接続) を選択します。

接続を完了することを選択し、接続が保留状態ではないというメッセージが表示された場合は、接続がすでに使用可能な状態になっているため、要求をキャンセルできます。

接続の GitClone アクセス許可を追加する

ソースアクションと CodeBuild アクションで AWS CodeStar 接続を使用する場合、入力アーティファクトをビルドに渡す方法は 2 つあります。

- デフォルト: ソースアクションは、 CodeBuild がダウンロードするコードを含む zip ファイルを生成します。
- Git クローン: ソースコードは、直接ビルド環境にダウンロードできます。

  Git クローンモードでは、作業中の Git リポジトリとしてソースコードを操作することができます。このモードを使用するには、接続を使用するためのアクセス許可を CodeBuild 環境 に付与する必要があります。

CodeBuild サービスのロールポリシーにアクセス許可を追加するには、CodeBuild サービスのロールにアタッチするカスタマーマネージドポリシーを作成します。次の手順では、`UseConnection` のアクセス許可が `action` フィールドに指定され、接続 Amazon Resource Name (ARN) が `Resource` フィールドに指定されたポリシーを作成します。

コンソールを使用して UseConnection のアクセス許可を追加するには

1. パイプラインの接続 ARN を確認するには、パイプラインを開き、ソースアクションの (i) のアイコンを選択します。[Configuration] (設定) ペインが開き、接続 ARN が [ConnectionArn] の横に表示されます。CodeBuild サービスロールポリシーに接続 ARN を追加します。
2. CodeBuild サービスロールを確認するには、パイプラインで使用されているビルドプロジェクトを開き、[Build details] (ビルドの詳細) タブに移動します。
3. [Environment] (環境) セクションで、[Service role] (サービスロール) リンクを選択します。これにより AWS Identity and Access Management (IAM) コンソールが開き、接続へのアクセスを許可する新しいポリシーを追加できます。
4. IAM コンソールで [ポリシーのアタッチ] を選択し、[ポリシーの作成] を選択します。

   次のサンプルポリシーテンプレートを使用します。次の例に示すように、`Resource` フィールドに接続 ARN を追加します。

   JSON

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

```
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "codestar-connections:UseConnection",
            "Resource": "arn:aws:iam::*:role/Service*"
        }
    ]
}
```

[JSON] タブで、ポリシーを貼り付けます。

5. [ポリシーの確認] を選択します。ポリシーの名前 (例: **connection-permissions**) を入力し、[ポリシーの作成] を選択します。
6. サービスロール Attach Permissions (アクセス許可のアタッチ) ページに戻り、ポリシーリストを更新して、作成したポリシーを選択します。ポリシーのアタッチ を選択します。

ホストが使用可能な状態ではありません

ホストが `Available` 状態ではないというメッセージがコンソールに表示される場合は、[Set up host] (ホストのセットアップ) を選択します。

ホスト作成の最初のステップにより、作成されたホストは `Pending` 状態になります。ホストを `Available` 状態に移行するには、コンソールでホストをセットアップすることを選択する必要があります。詳細については、「保留中のホストをセットアップする」を参照してください。

> **Note**
>
> CLI AWS を使用して`Pending`ホストをセットアップすることはできません。

接続エラーのあるホストのトラブルシューティング

基盤となる GitHub アプリが削除または変更された場合、接続とホストがエラー状態に移行する可能性があります。エラー状態のホストと接続はリカバリできず、ホストを再作成する必要があります。

- アプリの pem キーの変更、アプリ名の変更 (最初の作成後) などのアクションにより、ホストと関連するすべての接続がエラー状態になります。

コンソールまたは CLI がホストまたは `Error` 状態のホストに関連する接続を返す場合は、次の手順を実行する必要がある場合があります。

- ホストリソースを削除して再作成し、ホスト登録アプリを再インストールします。詳細については、「ホストを作成する」を参照してください。

ホストへの接続を作成できません

接続またはホストを作成するには、次の条件が必要です。

- ホストは AVAILABLE 状態である必要があります。詳細については、次を参照してください。
- 接続はホストと同じリージョンで作成する必要があります。

ホストの VPC 設定のトラブルシューティング

ホストリソースを作成するときは、GitHub Enterprise Server インスタンスがインストールされているインフラストラクチャのネットワーク接続または VPC 情報を提供する必要があります。ホストの VPC またはサブネット設定をトラブルシューティングするには、ここに示す VPC 情報の例を参考にしてください。

> **Note**
>
> このセクションは、Amazon VPC 内の GitHub Enterprise Server ホスト設定に関連するトラブルシューティングに使用します。VPC (PrivateLink) の ウェブフックエンドポイントを使用するように設定されている接続に関連するトラブルシューティングについては、「GitHub Enterprise Server 接続用の ウェブフック VPC エンドポイント (PrivateLink) のトラブルシューティング」を参照してください。

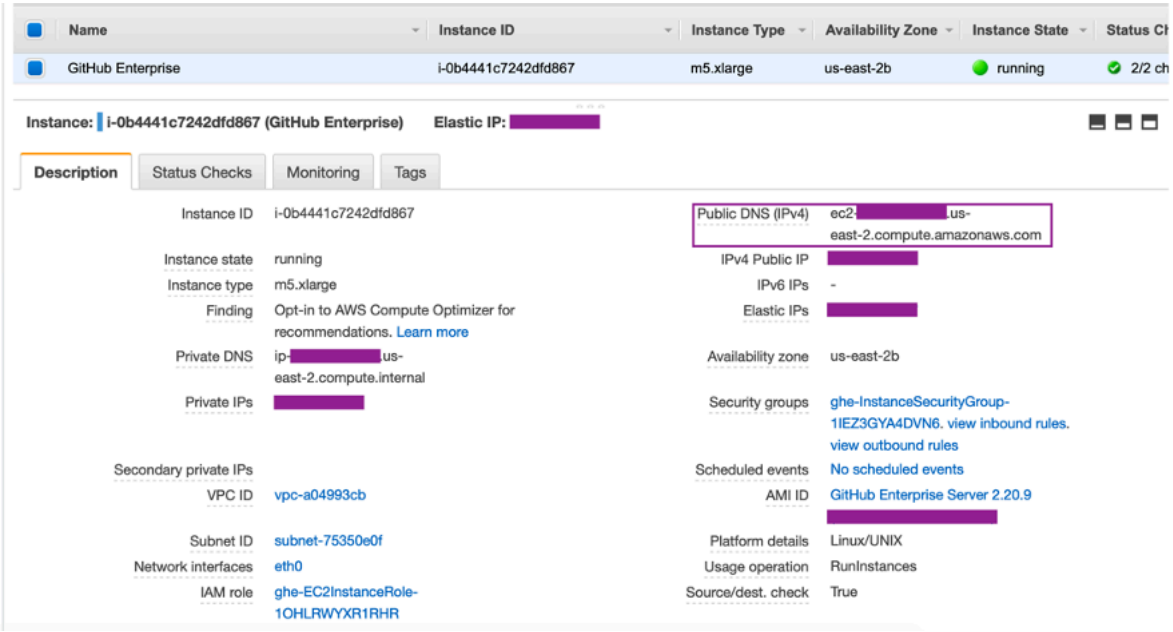
この例では、次のプロセスを使用して、GitHub Enterprise Server インスタンスをインストールする VPC とサーバーを設定します。

1. VPC を作成します。詳細については、「https://docs.aws.amazon.com/vpc/latest/userguide/working-with-vpcs.html#Create-VPC」を参照してください。
2. VPC にサブネットを作成する 詳細については、「https://docs.aws.amazon.com/vpc/latest/userguide/working-with-vpcs.html#AddaSubnet」を参照してください。

3. VPC でインスタンスを起動する 詳細については、「https://docs.aws.amazon.com/vpc/latest/userguide/working-with-vpcs.html#VPC_Launch_Instance」を参照してください。

> **Note**
>
> 各 VPC は、一度に 1 つのホスト (GitHub Enterprise Server インスタンス) にのみ関連付けることができます。

次の図は、GitHub Enterprise AMI を使用して起動された EC2 インスタンスを示しています。



GitHub Enterprise Server 接続に VPC を使用する場合、ホストをセットアップするときにインフラストラクチャに以下を提供する必要があります。

- VPC ID: GitHub Enterprise Server インスタンスがインストールされているサーバーの VPC、または VPN または Direct Connect を介してインストールされた GitHub Enterprise Server インスタンスにアクセスできる VPC。
- サブネット ID: GitHub Enterprise Server インスタンスがインストールされているサーバーのサブネット、または VPN または Direct Connect を介してインストールされた GitHub Enterprise Server インスタンスにアクセスできるサブネット。
- セキュリティグループ: GitHub Enterprise Server インスタンスがインストールされているサーバーのセキュリティグループ、または VPN またはDirect Connect を介してインストールされた GitHub Enterprise Server インスタンスにアクセスできるセキュリティグループ。

- エンドポイント: サーバーエンドポイントを準備して、次のステップに進みます。

VPC とサブネットの使用方法の詳細については、Amazon VPC ユーザーガイド の「IPv4 用の VPC とサブネットのサイズ設定」を参照してください。

トピック

保留状態のホストを取得できません

ホストが VPC_CONFIG_FAILEED_INTIONALITINATION の状態になった場合、ホスト用に選択した VPC、サブネット、またはセキュリティグループに問題がある可能性があります。

- VPC、サブネット、セキュリティグループは、すべて、ホストを作成するアカウントに属している必要があります。
- サブネットとセキュリティグループは、選択した VPC に属している必要があります。
- 提供される各サブネットは、異なるアベイラビリティーゾーンに存在する必要があります。
- ホストを作成するユーザーには、次の IAM アクセス許可が必要です。

```
ec2:CreateNetworkInterface
ec2:CreateTags
ec2:DescribeDhcpOptionsec2:DescribeNetworkInterfaces
ec2:DescribeSubnets
ec2:DeleteNetworkInterface
ec2:DescribeVpcs
ec2:CreateVpcEndpoint
ec2:DeleteVpcEndpoints
ec2:DescribeVpcEndpoints
```

利用可能な状態でホストを取得できません

ホストの CodeConnections アプリ設定を完了できない場合は、VPC 設定または GitHub Enterprise Server インスタンスに問題がある可能性があります。

- パブリック認証局を使用していない場合は、GitHub Enterprise インスタンスで使用される TLS 証明書をホストに提供する必要があります。TLS 証明書の値は、証明書のパブリックキーである必要があります。
- GitHub アプリケーションを作成するには、GitHub Enterprise Server インスタンスの管理者である必要があります。

接続/ホストが動作していて、現在動作を停止しています

接続/ホストが以前に動作していて、現在動作していない場合は、VPC の設定が変更されたか、GitHub アプリが変更されたことが原因である可能性があります。以下をチェックしてください:

- 接続用に作成したホストリソースにアタッチされたセキュリティグループが変更されたか、GitHub Enterprise Server にアクセスできなくなりました。CodeConnections には、GitHub Enterprise Server インスタンスに接続できるセキュリティグループが必要です。
- DNS サーバーの IP が最近変更されました。これを確認するには、接続用に作成したホストリソースで指定されている VPC にアタッチされている DHCP オプションをチェックします。最近 AmazonProvidedDNS からカスタム DNS サーバーに移動した場合、または新しいカスタム DNS サーバーの使用を開始した場合は、ホスト/接続が機能しなくなることに注意してください。これを修正するには、既存のホストを削除して再作成してください。これにより、最新の DNS 設定がデータベースに保存されます。
- ネットワーク ACL の設定が変更され、GitHub Enterprise Server インフラストラクチャが配置されているサブネットへの HTTP 接続は許可されなくなりました。
- GitHub Enterprise Server の CodeConnections アプリの設定が変更されました。URLs やアプリシークレットなどの設定を変更すると、インストールされている GitHub Enterprise Server インスタンスと CodeConnections 間の接続が切断される可能性があります。

ネットワークインターフェイスを削除できません

ネットワークインターフェイスを検出できない場合は、次の点を確認してください。

- CodeConnections によって作成されたネットワークインターフェイスは、ホストを削除することによってのみ削除できます。ユーザーが手動で削除することはできません。
- アクセス許可を持っている必要があります。

```
ec2:DescribeNetworkInterfaces
ec2:DeleteNetworkInterface
```

GitHub Enterprise Server 接続用の ウェブフック VPC エンドポイント (PrivateLink) のトラブルシューティング

VPC 設定でホストを作成すると、Webhook VPC エンドポイントが自動的に作成されます。

> **Note**
>
> このセクションは、VPC (PrivateLink) の ウェブフックエンドポイントを使用するように設定されている接続に関連するトラブルシューティングに使用します。Amazon VPC 内の GitHub Enterprise Server ホスト設定に関連するトラブルシューティングについては、「ホストの VPC 設定のトラブルシューティング」を参照してください。

インストールされたプロバイダータイプへの接続を作成し、サーバーが VPC 内に設定されていることを指定した場合、 AWS CodeConnections によってホストが作成され、ウェブフックの VPC エンドポイント (PrivateLink) が自動的に作成されます。これにより、ホストはウェブフックを介して Amazon ネットワーク経由で統合 AWS サービスにイベントデータを送信できます。詳細については、「AWS CodeConnections およびインターフェイス VPC エンドポイント (AWS PrivateLink)」を参照してください。

トピック

- ウェブフックVPC エンドポイントを削除できません

ウェブフックVPC エンドポイントを削除できません

AWS CodeConnections は、ホストのウェブフック VPC エンドポイントのライフサイクルを管理します。エンドポイントを削除する場合は、対応するホストリソースを削除して、削除する必要があります。

- CodeConnections によって作成されたウェブフック VPC エンドポイント (PrivateLink) は、ホストを削除することによってのみ削除できます。手動で削除することはできません。
- アクセス許可を持っている必要があります。

```
ec2:DescribeNetworkInterfaces
ec2:DeleteNetworkInterface
```

2020 年 11 月 24 日以前に作成されたホストのトラブルシューティング

2020 年 11 月 24 日現在、 AWS CodeConnections がホストを設定すると、追加の VPC エンドポイント (PrivateLink) サポートが設定されます。この更新の前に作成したホストについては、このトラブルシューティングのセクションを使用してください。

詳細については、「AWS CodeConnections およびインターフェイス VPC エンドポイント (AWS PrivateLink)」を参照してください。

トピック

- 2020 年 11 月 24 日 以前に作成したホストがあり、ウェブフックに VPC エンドポイント（ PrivateLink ）を使用したいと考えています
- 利用可能な状態（ VPC エラー ）のホストを取得できません

2020 年 11 月 24 日 以前に作成したホストがあり、ウェブフックに VPC エンドポイント（ PrivateLink ）を使用したいと考えています

GitHub Enterprise Server 用にホストを設定すると、ウェブフックエンドポイントが自動的に作成されます。接続で VPC PrivateLink ウェブフックエンドポイントが使用されるようになりました。2020 年 11 月 24 日より前にホストを作成し、VPC PrivateLink ウェブフックエンドポイントを使用する場合は、最初にホストを削除してから、新しいホストを作成する必要があります。

利用可能な状態（ VPC エラー ）のホストを取得できません

ホストが 2020 年 11 月 24 日より前に作成されていて、ホストの CodeConnections アプリ設定を完了できない場合、VPC 設定または GitHub Enterprise Server インスタンスに問題がある可能性があります。

GitHub Enterprise Server インスタンスが GitHub Webhook の出力ネットワークトラフィックを送信できるようにするために、VPC には NAT ゲートウェイ（ またはアウトバウンドインターネットアクセス ）が必要です。

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。

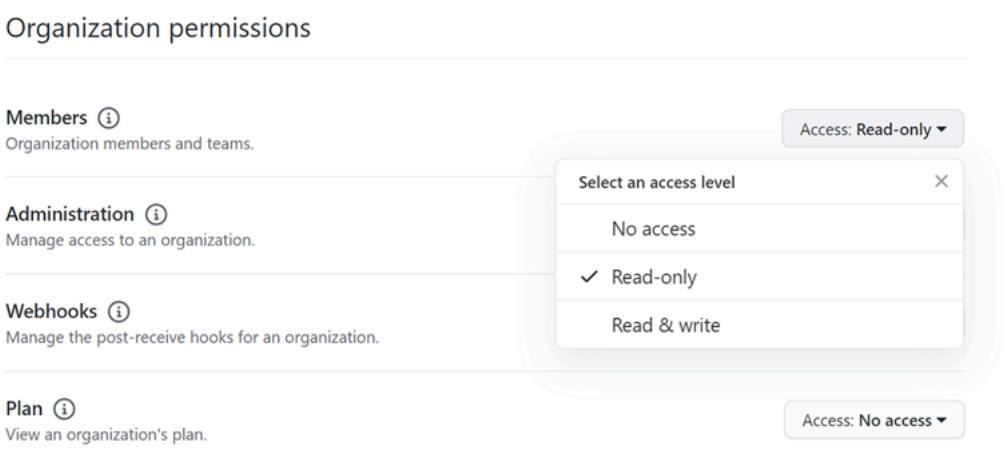
解決方法:GitHub リポジトリのアクセス許可レベルの詳細については、https://docs.github.com/en/free-pro-team@latest/github/setting-up-and-managing-organizations-and-teams/permission-levels-for-an-organization を参照してください。

GitHub Enterprise Server 接続アプリのアクセス許可を編集する

2020 年 12 月 23 日以前に GitHub Enterprise Server 用のアプリをインストールした場合、組織のメンバーはアプリ読み取り専用のアクセス許可が必要な場合があります。GitHub アプリの所有者である場合は、以下の手順に従って、ホストの作成時にインストールされたアプリのアクセス許可を編集します。

> **Note**
>
> GitHub Enterprise Server インスタンスでこれらの手順を完了し、GitHub アプリケーションの所有者になる必要があります。

1. GitHub Enterprise Serve で、プロフィール写真のドロップダウンオプションから、[Settings] (設定) を選択します。
2. [Developer settings] (開発者設定) を選択してから、GitHub Apps (GitHub アプリ) を選択します。
3. アプリの一覧で、接続するアプリの名前を選択し、[Permissions and events] (アクセス許可とイベント) 設定画面に表示されます。
4. [Organization permissions] (組織のアクセス許可) の [Members] (メンバー) で、[Access] (アクセス) ドロップダウンから [Read-only] (読み取り専用) を選択します。



5. [Add a note to users] (新しいクライアントを設定) で、更新の理由の説明を追加します。[Save changes] (変更の保存) をクリックします。

GitHub への接続時の接続エラー:「問題が発生しました。ブラウザで Cookie が有効になっていることを確認してください」または「組織の所有者は GitHub アプリケーションをインストールする必要があります」

問題:

GitHub リポジトリの接続を作成するには、GitHub 組織の所有者である必要があります。組織のリポジトリではない場合、ユーザーがリポジトリの所有者である必要があります。接続の作成者が組織の所有者以外である場合、組織の所有者へのリクエストが作成され、次のエラーのいずれかが表示されます。

問題が発生しました。ブラウザで Cookie が有効になっていることを確認してください

OR

組織の所有者は GitHub アプリケーションをインストールする必要があります

解決策: GitHub 組織のリポジトリである場合、組織の所有者が GitHub リポジトリへの接続を作成する必要があります。組織のリポジトリでない場合、ユーザーがリポジトリの所有者である必要があります。

IAM ポリシーでは、リソースの接続サービスプレフィックスを更新する必要がある場合があります

2024 年 3 月 29 日、サービスの名前が AWS CodeStar Connections から AWS CodeConnections に変更されました。2024 年 7 月 1 日以降、コンソールはリソース ARN `codeconnections`にとの接続を作成します。両方のサービスプレフィックスを持つリソースは、コンソールに引き続き表示されます。コンソールを使用して作成されたリソースのサービスプレフィックスは ですcodeconnections。新しい SDK/CLI リソースは、リソース ARN `codeconnections`で を使用して作成されます。作成されたリソースには、自動的に新しいサービスプレフィックスが付けられます。

以下は、 AWS CodeConnections で作成されるリソースです。

- Connections

- [ホスト]

問題:

ARN codestar-connectionsで を使用して作成されたリソースの名前は、リソース ARN の新しいサービスプレフィックスに自動的に変更されません。新しいリソースを作成すると、接続サービスのプレフィックスを持つリソースが作成されます。ただし、codestar-connectionsサービスプレフィックスを持つ IAM ポリシーは、新しいサービスプレフィックスを持つリソースでは機能しません。

解決方法: リソースのアクセスまたはアクセス許可の問題を回避するには、次のアクションを実行します。

- 新しいサービスプレフィックスの IAM ポリシーを更新します。そうしないと、名前を変更または作成したリソースは IAM ポリシーを使用できません。
- コンソールまたは CLI/CDK/CFN を使用して作成することで、新しいサービスプレフィックスのリソースを更新します。

必要に応じて、ポリシーのアクション、リソース、および条件を更新します。次の例では、両方のサービスプレフィックスの Resourceフィールドが更新されています。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Action": [
            "codeconnections:UseConnection"
        ],
        "Resource": [
            "arn:aws:codestar-connections:*:*:connection/*",
            "arn:aws:codeconnections:*:*:connection/*"
        ]
    }
}
```

コンソールを使用して作成されたリソースのサービスプレフィックスによるアクセス許可エラー

現在、コンソールを使用して作成された接続リソースには、codestar-connectionsサービスプレフィックスのみが含まれます。コンソールを使用して作成されたリソースの場合、ポリシーステートメントアクションにはサービスプレフィックスcodestar-connectionsとして を含める必要があります。

> **Note**
>
> 2024 年 7 月 1 日以降、コンソールはリソース ARN codeconnectionsに との接続を作成します。両方のサービスプレフィックスを持つリソースは、コンソールに引き続き表示されます。

問題:

コンソールを使用して接続リソースを作成する場合、codestar-connectionsサービスプレフィックスをポリシーで使用する必要があります。ポリシーでcodeconnectionsサービスプレフィックスを持つポリシーを使用すると、コンソールを使用して作成された接続リソースに次のエラーメッセージが表示されます。

```
User: user_ARN is not authorized to perform: codestar-connections:action on
 resource: resource_ARN because no identity-based policy allows the codestar-
connections:action action
```

解決方法: コンソールを使用して作成されたリソースの場合、 のポリシー例に示すように、ポリシーステートメントアクションにサービスプレフィックスcodestar-connectionsとして を含める必要があります例: コンソール AWS CodeConnections で を作成するためのポリシー。

組織をサポートするインストール済みプロバイダーの接続とホストのセットアップ

GitHub Organizations などの組織をサポートするインストール済みプロバイダーの場合、使用可能なホストを渡しません。組織内の接続ごとに新しいホストを作成し、次のネットワークフィールドに必ず同じ情報を入力します。

- VPC ID
- サブネット ID

- セキュリティグループ IDs

関連するステップを参照して、GHES 接続または GitLab セルフマネージド接続を作成します。

接続の制限を引き上げることはできますか

CodeConnections では、特定の制限の制限の引き上げをリクエストできます。詳細については、「接続のクォータ」を参照してください。

接続のクォータ

次の表に、デベロッパーツールコンソールでの接続のクォータ (制限) を示します。

この表のクォータは ごとに適用 AWS リージョン され、引き上げることができます。 AWS リージョン の情報と変更可能なクォータについては、「AWS のサービスクォータ」を参照してください。

> **Note**
>
> 使用 AWS リージョン する前に、欧州 (ミラノ) を有効にする必要があります。詳細については、「リージョンの有効化」を参照してください。

リソース	デフォルトの制限
あたりの接続の最大数 AWS アカウント	250

このテーブルのクォータは固定されており、変更できません。

リソース	デフォルトの制限
接続名の最大文字数	32 文字
あたりのホストの最大数 AWS アカウント	50
リポジトリリンクの最大数	100

リソース	デフォルトの制限
CloudFormation スタック同期設定の最大数	100
リポジトリリンクあたりの同期設定の最大数	100
ブランチあたりの同期設定の最大数	50

許可リストに追加する IP アドレス

IP フィルタリングを実装するか、Amazon EC2 インスタンスで特定の IP アドレスを許可する場合は、以下の IP アドレスを許可リストに追加します。これにより、GitHub や Bitbucket などのプロバイダーへの接続が可能になります。

次の表に、デベロッパーツールコンソールの接続用の IP アドレスを AWS リージョン別に一覧表示します。

> **Note**
>
> 欧州 (ミラノ) リージョンの場合、このリージョンを使用する前にリージョンを有効にする必要があります。詳細については、「リージョンの有効化」を参照してください。

リージョン	IP アドレス
米国西部 (オレゴン) (us-west-2)	35.160.210.199「」、「54.71.206.108」、「54.71.36.205」
米国東部 (バージニア北部) (us-east-1)	3. 216.216.90「」、「」、216.243.220「」、217.241.85「」
欧州 (アイルランド) (eu-west-1)	34. 242.64.82「」、「52.18.37.201」、「54.77.75.62」
米国東部 (オハイオ) (us-east-2)	18.217.188.190、18.218.158.91、18.220.4.80
アジアパシフィック (シンガポール) (ap-southeast-1)	18.138.171.151、18.139.22.70、3.1.157.176

リージョン	IP アドレス
アジアパシフィック (シドニー) (ap-south east-2)	13. 236.59.253「」、「52.64.166.86」、「54.206.1.112」
アジアパシフィック (東京) (ap-northeast-1)	52.196.132.231、54.95.133.227、18.181.13.91
ヨーロッパ (フランクフルト) (eu-central-1)	18.196.145.164、3.121.252.59、52.59.104.195
アジアパシフィック (ソウル) (ap-northeast-2)	13.125.8.239、13.209.223.177、3.37.200.23
アジアパシフィック (ムンバイ) (ap-south-1)	13. 234.199.152「」、13. 235.29.22 0「」、35. 154.230.124「」
南米 (サンパウロ) (sa-east-1)	18. 229.77.26「」、「54. 233.226.52」、「54. 233.207.69」
カナダ (中部) (ca-central-1)	15.222.219.210、35.182.166.138、99.79. 111.198
ヨーロッパ (ロンドン) (eu-west-2)	3.9.97205, 35.177.150.185, 35.177.200.225
米国西部 (北カリフォルニア) (us-west-1)	52.52.16.175、52.8.63.87
欧州 (パリ) (eu-west-3)	35. 181.127.138「」、「35. 181.145.22」、「35. 181.20.200」
欧州 (ストックホルム) (eu-north-1)	13.48.66.148、13.48.8.79、13.53.78.182
欧州 (ミラノ) (eu-south-1)	18.102.28.105、18.102.35.130、18.102.8.116
AWS GovCloud (米国東部)	18.252.168.157、18.252.207.77、18.253. 185.119

デベロッパーツールコンソールの機能のセキュリティ

のクラウドセキュリティが最優先事項 AWS です。お客様は AWS 、セキュリティを最も重視する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 お客様とお客様の間の責任共有です。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して説明しています。

- クラウドのセキュリティ – AWS クラウドで 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。「AWS 」 コンプライアンスプログラムの一環として、サードパーティーの監査が定期的にセキュリティの有効性をテストおよび検証しています。 AWS CodeStar Notifications と AWS CodeConnections に適用されるコンプライアンスプログラムについては、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。
- クラウドのセキュリティ – 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、 AWS CodeStar Notifications と AWS CodeConnections を使用する際に責任共有モデルを適用する方法を理解するのに役立ちます。以下のトピックでは、セキュリティおよびコンプライアンスの目的を達成するために AWS CodeStar Notifications と AWS CodeConnections を設定する方法について説明します。また、 AWS CodeStar Notifications および AWS CodeConnections リソースのモニタリングと保護に役立つ他の AWS サービスの使用方法についても説明します。

デベロッパーツールコンソールにおけるサービスのセキュリティについては、以下を参照してください。

- CodeBuild セキュリティ
- CodeCommit セキュリティ
- CodeDeploy セキュリティ
- CodePipeline セキュリティ

通知の内容とセキュリティについて

通知は、設定した通知ルールのターゲットにサブスクライブしているユーザーにリソースに関する情報を提供します。これには、リポジトリのコンテンツ、ビルドのステータス、デプロイのステータス、パイプラインの実行など、デベロッパーツールのリソースに関する情報が含まれます。

例えば、CodeCommit のリポジトリに対して通知ルールを設定し、コミットやプルリクエストに関するコメントを含めることができます。その場合、このルールに応答して送信される通知には、そのコメントで参照されているコード行が含まれる場合があります。同様に、CodeBuild のビルドプロジェクトに対して通知ルールを設定し、ビルドの状態やフェーズの成功または失敗を含めることができます。このルールに応答して送信される通知には、該当する情報が含まれます。

CodePipeline のパイプラインに対する通知ルールを設定し、手動承認に関する情報を含めることができます。このルールに応答して送信される通知には、その承認を提供するユーザーの名前が含まれる場合があります。CodeDeploy でのアプリケーションの通知ルールは、デプロイの成功を示すように設定でき、また、その規則に応答して送信される通知には、デプロイターゲットに関する情報が含まれる場合があります。

通知には、ビルドのステータス、コメントのあるコード行、デプロイのステータス、パイプラインの承認など、プロジェクト固有の情報が含まれます。プロジェクトのセキュリティを確保するために、通知ルールのターゲットと、ターゲットとして指定された Amazon SNS トピックの受信者のリストの両方を定期的に確認してください。さらに、イベントに応答して送信される通知の内容は、基盤となるサービスに機能が追加されると、変わる場合があります。この変更は、既存の通知ルールへの予告なしに発生する可能性があります。通知メッセージの内容を定期的に確認して、送信内容と送信先のユーザーを確認してください。

通知ルールで使用できるイベントタイプの詳細については、「通知の概念」を参照してください。

通知に含まれる詳細を、イベントに含まれるもののみに制限するように選択できます。これは、ベーシック詳細タイプと呼ばれます。これらのイベントには、Amazon EventBridge および Amazon CloudWatch Events に送信される情報とまったく同じ情報が含まれます。

CodeCommit などのデベロッパーツールコンソールのサービスは、イベントで使用できる以外のイベントタイプの一部またはすべての情報を通知メッセージに追加することを選択する場合があります。この補足情報は、現在のイベントタイプを強化、または将来のイベントタイプを補足するためにいつでも追加できます。[Full (完全)] 詳細タイプを選択して、イベントに関する補足情報 (使用可能な場合) を通知に含めることができます。詳細については、「詳細タイプ」を参照してください。

AWS CodeStar Notifications および AWS CodeConnections でのデータ保護

責任 AWS 共有モデル、 AWS CodeStar Notifications および AWS CodeConnections 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。CloudTrail 証跡を使用して AWS アクティビティをキャプチャする方法については、「 AWS CloudTrail ユーザーガイド」のCloudTrail 証跡の使用」を参照してください。
- 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 AWS CodeStar Notifications および AWS CodeConnections AWS CLIまたは他の AWS のサービス を使用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。

AWS CodeStar Notifications と AWS CodeConnections 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 Notifications および AWS CodeConnections リソースの使用を許可する (アクセス許可を付与する) かを制御します。IAM は、追加料金なしで使用できる AWS のサービス です。

> **Note**
>
> 新しいサービスプレフィックスで作成されたリソースのアクションcodeconnectionsを使用できます。新しいサービスプレフィックスでリソースを作成すると、リソース ARN codeconnectionsで が使用されます。codestar-connections サービスプレフィックスのアクションとリソースは引き続き使用できます。IAM ポリシーでリソースを指定する場合、サービスプレフィックスはリソースのプレフィックスと一致する必要があります。

トピック

- オーディエンス
- アイデンティティを使用した認証
- ポリシーを使用したアクセスの管理
- デベロッパーツールコンソールの機能と IAM との連携方法
- AWS CodeConnections アクセス許可リファレンス
- アイデンティティベースのポリシーの例
- タグを使用して AWS CodeConnections リソースへのアクセスを制御する
- コンソールでの通知と接続の使用
- ユーザーが自分の許可を表示できるようにする
- AWS CodeStar Notifications と AWS CodeConnections 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
- AWS CodeStar Notifications のサービスにリンクされたロールの使用

- のサービスにリンクされたロールの使用 AWS CodeConnections
- AWS の 管理ポリシー AWS CodeConnections

オーディエンス

AWS Identity and Access Management (IAM) の使用方法は、ロールによって異なります。

- サービスユーザー - 機能にアクセスできない場合は、管理者にアクセス許可をリクエストします (「AWS CodeStar Notifications と AWS CodeConnections 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)。
- サービス管理者 - ユーザーアクセスを決定し、アクセス許可リクエストを送信します (「デベロッパーツールコンソールの機能と IAM との連携方法」を参照)
- IAM 管理者 - アクセスを管理するためのポリシーを作成します (「アイデンティティベースのポリシーの例」を参照)

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。、IAM ユーザー 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で認証される必要があります。

AWS IAM アイデンティティセンター (IAM Identity Center)、シングルサインオン認証、Google/Facebook 認証情報などの ID ソースからの認証情報を使用して、フェデレーティッド ID としてサインインできます。サインインの詳細については、「AWS サインイン ユーザーガイド」の「AWS アカウントにサインインする方法」を参照してください。

プログラムによるアクセスの場合、 は SDK と CLI AWS を提供してリクエストを暗号化して署名します。詳細については、「IAM ユーザーガイド」の「API リクエストに対するAWS 署名バージョン 4」を参照してください。

AWS アカウントのルートユーザー

を作成するときは AWS アカウント、すべての AWS のサービス および リソースへの完全なアクセス権を持つ AWS アカウント ルートユーザーと呼ばれる 1 つのサインインアイデンティティから始めます。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。ルートユーザー認証情報を必要とするタスクについては、「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、特定の個人やアプリケーションに対する特定のアクセス許可を持つアイデンティティです。長期認証情報を持つ IAM ユーザーの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。詳細については、IAM ユーザーガイドの「ID プロバイダーとのフェデレーションを使用して にアクセスする必要がある AWS」を参照してください。

IAM グループは、IAM ユーザーの集合を指定し、大量のユーザーに対するアクセス許可の管理を容易にします。詳細については、「IAM ユーザーガイド」の「IAM ユーザーに関するユースケース」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を持つアイデンティであり、一時的な認証情報を提供します。ユーザーから IAM ロール (コンソール) に切り替えるか、 または API オペレーションを呼び出すことで、ロールを引き受けることができます。 AWS CLI AWS 詳細については、「IAM ユーザーガイド」の「ロールを引き受けるための各種方法」を参照してください。

IAM ロールは、フェデレーションユーザーアクセス、一時的な IAM ユーザーのアクセス許可、クロスアカウントアクセス、クロスサービスアクセス、および Amazon EC2 で実行するアプリケーションに役立ちます。詳細については、IAM ユーザーガイド の IAM でのクロスアカウントリソースアクセス 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、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場合のアクセス許可を定義します。 は、プリンシパル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。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、ポリシーを使用して、どのプリンシパルがどのリソースに対して、どのような条件でアクションを実行できるかを定義することで、誰が何にアクセスできるかを指定します。

デフォルトでは、ユーザーやロールにアクセス許可はありません。IAM 管理者は IAM ポリシーを作成してロールに追加し、このロールをユーザーが引き受けられるようにします。IAM ポリシーは、オペレーションの実行方法を問わず、アクセス許可を定義します。

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のポリシーは、アイデンティティ (ユーザー、グループ、またはロール) にアタッチできる JSON アクセス許可ポリシードキュメントです。これらのポリシーは、アイデンティティがどのリソースに対してどのような条件下でどのようなアクションを実行できるかを制御します。アイデンティティベースポリシーの作成方法については、IAM ユーザーガイド の カスタマー管理ポリシーでカスタム IAM アクセス許可を定義する 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、インラインポリシー (単一の ID に直接埋め込む) または管理ポリシー (複数の ID にアタッチされたスタンドアロンポリシー) にすることができます。管理ポリシーと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「管理ポリシーとインラインポリシーのいずれかを選択する」を参照してください。

デベロッパーツールコンソールの機能と IAM との連携方法

IAM を使用してデベロッパーツールコンソールの機能へのアクセスを管理する前に、どの IAM 機能を使用できるかを理解する必要があります。通知やその他の AWS 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

- デベロッパーツールコンソールにおける通知のアイデンティティベースのポリシー
- AWS CodeStar Notifications および AWS CodeConnections リソースベースのポリシー
- タグに基づく認可
- IAM ロール

デベロッパーツールコンソールにおける通知の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するアクションとリソース、またアクションを許可または拒否する条件を指定できます。 AWS CodeStar Notifications と AWS CodeConnections 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 ポリシーエレメントのリファレンス」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。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。

デベロッパーツールコンソールでの通知のポリシーアクションは、アクション の前にプレフィックス codestar-notifications and codeconnections を使用します。例えば、アカウント内のすべての通知ルールを表示するアクセス許可をユーザーに付与するには、そのユーザーのポリシーに codestar-notifications:ListNotificationRules アクションを含めます。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 Notifications と AWS CodeConnections 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。

1 つのステートメントで複数の AWS CodeStar Notifications アクションを指定するには、次のようにカンマで区切ります。

```
"Action": [
      "codestar-notifications:action1",
      "codestar-notifications:action2"
```

1 つのステートメントで複数の AWS CodeConnections アクションを指定するには、次のようにカンマで区切ります。

```
"Action": [
      "codeconnections:action1",
      "codeconnections:action2"
```

ワイルドカード *を使用して複数のアクションを指定することができます。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-notifications:List*"
```

AWS CodeStar Notifications API アクションには以下が含まれます。

- CreateNotificationRule
- DeleteNotificationRule
- DeleteTarget
- DescribeNotificationRule
- ListEventTypes
- ListNotificationRules
- ListTagsForResource
- ListTargets
- Subscribe
- TagResource
- Unsubscribe
- UntagResource
- UpdateNotificationRule

AWS CodeConnections API アクションには以下が含まれます。

- CreateConnection
- DeleteConnection
- GetConnection
- ListConnections
- ListTagsForResource
- TagResource
- UntagResource

認証ハンドシェイクを完了する AWS CodeConnections には、 で次のアクセス許可のみのアクションが必要です。

- GetIndividualAccessToken
- GetInstallationUrl
- ListInstallationTargets
- StartOAuthHandshake
- UpdateConnectionInstallation

接続を使用するには AWS CodeConnections 、 で次のアクセス許可のみのアクションが必要です。

- `UseConnection`

サービスへの接続を渡す AWS CodeConnections には、 で次のアクセス許可のみのアクションが必要です。

- `PassConnection`

AWS CodeStar Notifications および AWS CodeConnections アクションのリストを確認するには、IAM ユーザーガイドのAWS CodeStar Notifications で定義されるアクション」およびAWS CodeConnections で定義されるアクション」を参照してください。

リソース

AWS CodeStar Notifications と AWS CodeConnections は、ポリシーでのリソース ARNs の指定をサポートしていません。

条件キー

AWS CodeStar Notifications と AWS CodeConnections は、独自の条件キーのセットを定義し、一部のグローバル条件キーの使用もサポートします。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。

All AWS CodeStar Notifications アクションは、 `codestar-notifications:NotificationsForResource` 条件キーをサポートします。詳細については、「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 CodeConnections は、IAM ポリシーの `Condition`要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。詳細については、「AWS CodeConnections アクセス許可リファレンス」を参照してください。

条件キー	説明
`codeconnections:BranchName`	サードパーティーリポジトリのブランチ名でアクセスをフィルタリングします

条件キー	説明
codeconnections:FullRepositoryId	リクエストで渡されたリポジトリによるアクセスをフィルタリングします。特定のリポジトリにアクセスするための UseConnection リクエストにのみ適用します
codeconnections:InstallationId	接続の更新に使用されるサードパーティー ID (Bitbucket アプリのインストール ID など) でアクセスをフィルタリングします。接続を作成するために使用できるサードパーティー製アプリのインストールを制限できます。
codeconnections:OwnerId	サードパーティープロバイダーの所有者またはアカウント ID でアクセスをフィルタリングします
codeconnections:PassedToService	プリンシパルが接続を渡すことができるサービスでアクセスをフィルタリングします
codeconnections:ProviderAction	ListRepositories など、UseConnection リクエストのプロバイダーアクションでアクセスをフィルタリングします。
codeconnections:ProviderPermissionsRequired	サードパーティープロバイダーのアクセス許可のタイプでアクセスをフィルタリングします
codeconnections:ProviderType	リクエストで渡されたサードパーティープロバイダーのタイプによってアクセスをフィルタリングします。
codeconnections:ProviderTypeFilter	結果をフィルタリングするために使用されるサードパーティープロバイダーのタイプによってアクセスをフィルタリングします。
codeconnections:RepositoryName	サードパーティーのリポジトリ名でアクセスをフィルタリングします

例

AWS CodeStar Notifications と AWS CodeConnections 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アイデンティティベースのポリシーの例。

AWS CodeStar Notifications および AWS CodeConnections リソースベースのポリシー

AWS CodeStar Notifications と AWS CodeConnections は、リソースベースのポリシーをサポートしていません。

タグに基づく認可

AWS CodeStar Notifications および AWS CodeConnections リソースにタグをアタッチすることも、リクエストでタグを渡すこともできます。タグに基づいてアクセスを管理するには、`codestar-notifications and codeconnections:ResourceTag/`*`key-name`*、`aws:RequestTag/`*`key-name`*、または `aws:TagKeys` の条件キーを使用して、ポリシーの条件要素でタグ情報を提供します。タグ付け戦略の詳細については、「 AWS リソースのタグ付け」を参照してください。 AWS CodeStar Notifications および AWS CodeConnections リソースのタグ付けの詳細については、「」を参照してくださいタグ接続リソース。

リソースのタグに基づいてリソース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、「タグを使用して AWS CodeConnections リソースへのアクセスを制御する」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を持つ AWS アカウント内のエンティティです。

一時的な認証情報を使用する

一時的な認証情報を使用して、フェデレーションでのサインイン、 IAM ロールの引き受け、またはクロスアカウントロールの引き受けを行うことができます。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 Notifications と AWS CodeConnections は、一時的な認証情報の使用をサポートしています。

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。IAM 管理者は、サービスリンクロールの許可を表示できますが、編集することはできません。

AWS CodeStar Notifications は、サービスにリンクされたロールをサポートしています。 AWS CodeStar Notifications および AWS CodeConnections サービスにリンクされたロールの作成または管理の詳細については、「」を参照してくださいAWS CodeStar Notifications のサービスにリンクされたロールの使用。

CodeConnections 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。

AWS CodeConnections アクセス許可リファレンス

次の表に、各 AWS CodeConnections API オペレーション、アクセス許可を付与できる対応するアクション、およびアクセス許可を付与するために使用するリソース ARN の形式を示します。 AWS CodeConnections APIsは、その API で許可されるアクションの範囲に基づいてテーブルにグループ化されます。IAM アイデンティティ (アイデンティティベースのポリシー) にアタッチできるアクセス許可ポリシーを作成する際、参照してください。

アクセス許可ポリシーを作成するときに、ポリシーの `Action` フィールドでアクションを指定します。ポリシーの `Resource` フィールドで、ワイルドカード文字 (*) を使用して、または使用せずに、ARN としてリソース値を指定します。

接続ポリシーで条件を示すには、ここで説明され、条件キー に一覧表示されている条件キーを使用します。 AWS全体の条件キーを使用することもできます。 AWS全体のキーの完全なリストについては、IAM ユーザーガイドの「使用可能なキー」を参照してください。

アクションを指定するには、API オペレーション名 (例えば、`codeconnections` や `codeconnections:ListConnections`) の前に `codeconnections:CreateConnection` プレフィックスを使用します。

ワイルドカードの使用

複数のアクションまたはリソースを指定するには、ARN でワイルドカード文字 (*) を使用します。たとえば、 `codeconnections:*`は all AWS CodeConnections アクションを指定し、 という単語で始まる all AWS CodeConnections アクション`codeconnections:Get*`を指定しますGet。次の例では、`MyConnection` で始まる名前のすべてのリソースへのアクセスを許可します。

```
arn:aws:codeconnections:us-west-2:account-ID:connection/*
```

次のテーブルに示されている *##*リソースでのみワイルドカードを使用できます。ワイルドカードを *region* または *account-id* リソースで使用することはできません。ワイルドカードの詳細については、IAM ユーザーガイドの IAM ID を参照してください。

トピック

- 接続を管理するアクセス許可
- ホストを管理するためのアクセス許可
- 接続を完了するためのアクセス許可
- ホスト設定のアクセス許可
- サービスに接続を渡す
- 接続の使用
- ProviderAction でサポートされるアクセスタイプ
- 接続リソースにタグ付けするためにサポートされているアクセス許可
- リポジトリリンクに接続を渡す
- リポジトリリンクでサポートされる条件キー
- 接続共有でサポートされているアクセス許可

接続を管理するアクセス許可

AWS CLI または SDK を使用して接続を表示、作成、または削除するように指定されたロールまたはユーザーには、以下に制限されたアクセス許可が必要です。

> **Note**
>
> 次のアクセス許可のみでは、コンソールでの接続を完了または使用することはできません。接続を完了するためのアクセス許可 でアクセス許可を追加する必要があります。

```
codeconnections:CreateConnection
codeconnections:DeleteConnection
codeconnections:GetConnection
codeconnections:ListConnections
```

AWS CodeStar Notifications と AWS CodeConnections が接続を管理するためのアクションに必要なアクセス許可

CreateConnection

アクション:codeconnections:CreateConnection

CLI またはコンソールを使用して接続を作成するために必要です。

リソース:arn:aws:codeconnections:*region*:*account-id*:connection/*connection-id*

DeleteConnection

アクション:codeconnections:DeleteConnection

CLI またはコンソールを使用して接続を削除するために必要です。

リソース:arn:aws:codeconnections:*region*:*account-id*:connection/*connection-id*

GetConnection

アクション:codeconnections:GetConnection

CLI またはコンソールを使用して接続の詳細を表示するために必要です。

リソース:arn:aws:codeconnections:*region*:*account-id*:connection/*connection-id*

ListConnections

アクション:codeconnections:ListConnections

CLI またはコンソールを使用してアカウント内のすべての接続を一覧表示するために必要です。

リソース:arn:aws:codeconnections:*region*:*account-id*:connection/*connection-id*

これらのオペレーションでは、次の条件キーがサポートされます。

Action	条件キー
codeconnections:CreateConnection	codeconnections:ProviderType

Action	条件キー
codeconnections:DeleteConnection	該当なし
codeconnections:GetConnection	該当なし
codeconnections:ListConnections	codeconnections:ProviderTypeFilter

ホストを管理するためのアクセス許可

AWS CLI または SDK を使用してホストを表示、作成、または削除するように指定されたロールまたはユーザーには、以下に制限されたアクセス許可が必要です。

> **Note**
>
> 次のアクセス許可のみでは、ホストでの接続を完了または使用することはできません。ホスト設定のアクセス許可 でアクセス許可を追加する必要があります。

```
codeconnections:CreateHost
codeconnections:DeleteHost
codeconnections:GetHost
codeconnections:ListHosts
```

AWS CodeStar Notifications と AWS CodeConnections がホストを管理するためのアクションに必要なアクセス許可

CreateHost

アクション:codeconnections:CreateHost

CLI またはコンソールを使用してホストを作成するために必要です。

リソース:arn:aws:codeconnections:*region*:*account-id*:host/*host-id*

DeleteHost

アクション:codeconnections:DeleteHost

CLI またはコンソールを使用してホストを削除するために必要です。

リソース:arn:aws:codeconnections:*region*:*account-id*:host/*host-id*

GetHost

アクション:codeconnections:GetHost

CLI またはコンソールを使用してホストの詳細を表示するために必要です。

リソース:arn:aws:codeconnections:*region*:*account-id*:host/*host-id*

ListHosts

アクション:codeconnections:ListHosts

CLI またはコンソールを使用してアカウント内のすべてのホストを一覧表示するために必要です。

リソース:arn:aws:codeconnections:*region*:*account-id*:host/*host-id*

これらのオペレーションでは、次の条件キーがサポートされます。

Action	条件キー
codeconnections:CreateHost	codeconnections:ProviderType codeconnections:VpcId
codeconnections:DeleteHost	該当なし
codeconnections:GetHost	該当なし
codeconnections:ListHosts	codeconnections:ProviderTypeFilter

VpcId 条件キーを使用するポリシーの例については、「」を参照してください例: VpcId コンテキストキーを使用してホスト VPC アクセス許可を制限する。

接続を完了するためのアクセス許可

コンソールで接続を管理するように指定されたロールまたはユーザーは、コンソールで接続を完了し、インストールを作成するために必要なアクセス許可を持っている必要があります。これには、プ

ロバイダーへのハンドシェイクの許可と、使用する接続用のインストールの作成が含まれます。上記のアクセス許可に加えて、次のアクセス許可を使用します。

ブラウザベースのハンドシェイクを実行する際に、コンソールは、次の IAM オペレーションを使用しま
す。ListInstallationTargets、GetInstallationUrl、StartOAuthHandshake、UpdateConnec
は IAM ポリシーアクセス許可です。API アクションではありません。

```
codeconnections:GetIndividualAccessToken
codeconnections:GetInstallationUrl
codeconnections:ListInstallationTargets
codeconnections:StartOAuthHandshake
codeconnections:UpdateConnectionInstallation
```

これに基づいて、コンソールで接続を使用、作成、更新、または削除するには、次のアクセス許可が必要です。

```
codeconnections:CreateConnection
codeconnections:DeleteConnection
codeconnections:GetConnection
codeconnections:ListConnections
codeconnections:UseConnection
codeconnections:ListInstallationTargets
codeconnections:GetInstallationUrl
codeconnections:StartOAuthHandshake
codeconnections:UpdateConnectionInstallation
codeconnections:GetIndividualAccessToken
```

AWS CodeConnections が接続を完了するためのアクションに必要なアクセス許可

GetIndividualAccessToken

アクション:codeconnections:GetIndividualAccessToken

コンソールを使用して接続を完了するために必要です。これは単なる IAM ポリシーのアクセス許可であり、API アクションではありません。

リソース:arn:aws:codeconnections:*region*:*account-id*:connection/*connection-id*

GetInstallationUrl

アクション:codeconnections:GetInstallationUrl

コンソールを使用して接続を完了するために必要です。これは単なる IAM ポリシーのアクセス許可であり、API アクションではありません。

リソース:arn:aws:codeconnections:*region*:*account-id*:connection/*connection-id*

ListInstallationTargets

アクション:codeconnections:ListInstallationTargets

コンソールを使用して接続を完了するために必要です。これは単なる IAM ポリシーのアクセス許可であり、API アクションではありません。

リソース:arn:aws:codeconnections:*region*:*account-id*:connection/*connection-id*

StartOAuthHandshake

アクション:codeconnections:StartOAuthHandshake

コンソールを使用して接続を完了するために必要です。これは単なる IAM ポリシーのアクセス許可であり、API アクションではありません。

リソース:arn:aws:codeconnections:*region*:*account-id*:connection/*connection-id*

UpdateConnectionInstallation

アクション:codeconnections:UpdateConnectionInstallation

コンソールを使用して接続を完了するために必要です。これは単なる IAM ポリシーのアクセス許可であり、API アクションではありません。

リソース:arn:aws:codeconnections:*region*:*account-id*:connection/*connection-id*

これらのオペレーションでは、次の条件キーがサポートされます。

Action	条件キー
codeconnections:GetIndividualAccessToken	codeconnections:ProviderType

Action	条件キー
codeconnections:GetInstallationUrl	codeconnections:ProviderType
codeconnections:ListInstallationTargets	該当なし
codeconnections:StartOAuthHandshake	codeconnections:ProviderType
codeconnections:UpdateConnectionInstallation	codeconnections:InstallationId

ホスト設定のアクセス許可

コンソールで接続を管理するように指定されたロールまたはユーザーは、コンソールでホストをセットアップするために必要なアクセス許可が必要です。これには、プロバイダーへのハンドシェイクの許可とホストアプリのインストールが含まれます。上記のホストのアクセス許可に加えて、次のアクセス許可を使用します。

ブラウザベースのホスト登録を実行するときに、次の IAM オペレーションがコンソールで使用されます。RegisterAppCode および StartAppRegistrationHandshake は IAM ポリシーのアクセス許可です。API アクションではありません。

```
codeconnections:RegisterAppCode
codeconnections:StartAppRegistrationHandshake
```

これに基づき、以下のアクセス許可を使用して、コンソールでホストを必要とする接続 (インストール済プロバイダータイプなど) を使用、作成、更新、または削除します。

```
codeconnections:CreateConnection
codeconnections:DeleteConnection
codeconnections:GetConnection
codeconnections:ListConnections
codeconnections:UseConnection
codeconnections:ListInstallationTargets
codeconnections:GetInstallationUrl
```

```
codeconnections:StartOAuthHandshake
codeconnections:UpdateConnectionInstallation
codeconnections:GetIndividualAccessToken
codeconnections:RegisterAppCode
codeconnections:StartAppRegistrationHandshake
```

AWS CodeConnections でホストのセットアップを完了するためのアクションに必要なアクセス許可

RegisterAppCode

アクション:codeconnections:RegisterAppCode

コンソールを使用してホストのセットアップを完了するために必要です。これは単なる IAM ポリシーのアクセス許可であり、API アクションではありません。

リソース:arn:aws:codeconnections:*region*:*account-id*:host/*host-id*

StartAppRegistrationHandshake

アクション:codeconnections:StartAppRegistrationHandshake

コンソールを使用してホストのセットアップを完了するために必要です。これは単なる IAM ポリシーのアクセス許可であり、API アクションではありません。

リソース:arn:aws:codeconnections:*region*:*account-id*:host/*host-id*

これらのオペレーションでは、次の条件キーがサポートされます。

サービスに接続を渡す

サービスに接続を渡す際 (例えば、パイプラインを作成または更新するためにパイプライン定義で接続 ARN が提供されるなど)、ユーザーには codeconnections:PassConnection のアクセス許可が必要です。

AWS CodeConnections が接続を渡すために必要なアクセス許可

PassConnection

アクション:codeconnections:PassConnection

サービスに接続を渡すために必要です。

リソース:arn:aws:codeconnections:*region*:*account-id*:connection/*connection-id*

このオペレーションでは、次の条件キーもサポートされます。

- codeconnections:PassedToService

条件キーでサポートされる値

Key	有効なアクションプロバイダー
codeconnections:PassedToService	• codeguru-reviewer • codepipeline.amazonaws.com • proton.amazonaws.com

接続の使用

CodePipeline のようなサービスが接続を使用する場合、サービスロールは特定の接続に対する codeconnections:UseConnection のアクセス許可を持っている必要があります。

コンソールで接続を管理するには、ユーザーポリシーに codeconnections:UseConnection アクセス許可が必要です。

AWS 接続を使用するために必要な CodeConnections アクション

UseConnection

アクション:codeconnections:UseConnection

接続を使用するために必要です。

リソース:arn:aws:codeconnections:*region*:*account-id*:connection/*connection-id*

このオペレーションでは、次の条件キーもサポートされます。

- codeconnections:BranchName
- codeconnections:FullRepositoryId
- codeconnections:OwnerId
- codeconnections:ProviderAction

- codeconnections:ProviderPermissionsRequired
- codeconnections:RepositoryName

条件キーでサポートされる値

Key	有効なアクションプロバイダー
codeconnections:FullRepositoryId	ユーザー名とリポジトリ名 (my-owner/my-repository など)。接続を使用して特定のリポジトリにアクセスする場合のみサポートされます。
codeconnections:ProviderPermissionsRequired	read_only または read_write
codeconnections:ProviderAction	GetBranch , ListRepositories , ListOwners , ListBranches , StartUploadArchiveToS3 , GitPush, GitPull, GetUploadArchiveToS3Status , CreatePullRequestDiffComment , GetPullRequest , ListBranchCommits , ListCommitFiles , ListPullRequestComments , ListPullRequestCommits . 詳細については、次のセクションをご覧ください。

一部の機能に必要な条件キーは、時間の経過とともに変化する可能性があります。アクセスコントロールの要件で、異なるアクセス許可が必要でない限り、codeconnections:UseConnection を使用して接続へのアクセスを制御することをお勧めします。

ProviderAction でサポートされるアクセスタイプ

AWS サービスで接続を使用すると、ソースコードプロバイダーに対して API コールが行われます。例えば、https://api.bitbucket.org/2.0/repositories/*username* API をコールすることによって、サービスは、Bitbucket 接続のリポジトリを一覧表示できます。

ProviderAction 条件キーを使用すると、プロバイダのどの API をコールすることができるかを制限できます。API パスは動的に生成される場合があり、パスはプロバイダーによって異なるため、ProviderAction 値は API の URL ではなく抽象アクション名にマッピングされます。これにより、接続のプロバイダーの種類に関係なく、同じ効果を持つポリシーを書くことができます。

サポートされている各 ProviderAction 値に対して許可されるアクセスタイプは次のとおりです。以下は IAM ポリシーアクセス許可です。API アクションではありません。

AWS で CodeConnections がサポートするアクセスタイプ **ProviderAction**

GetBranch

アクション:codeconnections:GetBranch

ブランチの最新のコミットなど、ブランチに関する情報にアクセスするために必要です。

リソース:arn:aws:codeconnections:*region*:*account-id*:connection/*connection-id*

ListRepositories

アクション:codeconnections:ListRepositories

所有者に属する公開および非公開リポジトリーのリストにアクセスするために必要です。

リソース:arn:aws:codeconnections:*region*:*account-id*:connection/*connection-id*

ListOwners

アクション:codeconnections:ListOwners

接続がアクセスできる所有者のリストにアクセスするために必要です。

リソース:arn:aws:codeconnections:*region*:*account-id*:connection/*connection-id*

ListBranches

アクション: codeconnections:ListBranches

指定したリポジトリに存在するブランチのリストにアクセスするために必要です。

リソース:arn:aws:codeconnections:*region*:*account-id*:connection/*connection-id*

StartUploadArchiveToS3

アクション:codeconnections:StartUploadArchiveToS3

ソースコードを読み取り、Amazon S3 にアップロードするために必要です。

リソース:arn:aws:codeconnections:*region*:*account-id*:connection/*connection-id*

GitPush

アクション: codeconnections:GitPush

Git を使用してリポジトリに書き込むために必要です。

リソース:arn:aws:codeconnections:*region*:*account-id*:connection/*connection-id*

GitPull

アクション: codeconnections:GitPull

Git を使用してリポジトリから読み込むために必要です。

リソース:arn:aws:codeconnections:*region*:*account-id*:connection/*connection-id*

GetUploadArchiveTos3Status

アクション:codeconnections:GetUploadArchiveToS3Status

StartUploadArchiveToS3 で始まるエラーメッセージを含む、アップロードのステータスにアクセスするために必要です。

リソース:arn:aws:codeconnections:*region*:*account-id*:connection/*connection-id*

CreatePullRequestDiffComment

アクション:codeconnections:CreatePullRequestDiffComment

プルリクエストのコメントにアクセスするために必要です。

リソース:arn:aws:codeconnections:*region*:*account-id*:connection/*connection-id*

GetPullRequest

アクション: codeconnections:GetPullRequest

リポジトリのプルリクエストを表示するために必要です。

リソース:arn:aws:codeconnections:*region*:*account-id*:connection/*connection-id*

ListBranchCommits

アクション:codeconnections:ListBranchCommits

リポジトリブランチのコミットのリストを表示するために必要です。

リソース:arn:aws:codeconnections:*region*:*account-id*:connection/*connection-id*

ListCommitFiles

アクション:codeconnections:ListCommitFiles

コミットのファイルのリストを表示するために必要です。

リソース:arn:aws:codeconnections:*region*:*account-id*:connection/*connection-id*

ListPullRequestComments

アクション:codeconnections:ListPullRequestComments

プルリクエストのコメントのリストを表示するために必要です。

リソース:arn:aws:codeconnections:*region*:*account-id*:connection/*connection-id*

ListPullRequestCommits

アクション:codeconnections:ListPullRequestCommits

プルリクエストのコミットのリストを表示するために必要です。

リソース:arn:aws:codeconnections:*region*:*account-id*:connection/*connection-id*

接続リソースにタグ付けするためにサポートされているアクセス許可

次の IAM オペレーションは、接続リソースをタグ付けするときに使用されます。

```
codeconnections:ListTagsForResource
codeconnections:TagResource
codeconnections:UntagResource
```

AWS CodeConnections で接続リソースにタグ付けするために必要なアクション

ListTagsForResource

アクション:codeconnections:ListTagsForResource

接続リソースに関連付けられているタグのリストを表示するために必要です。

リソース:arn:aws:codeconnections:*region*:*account-id*:connection/*connection-id*、 arn:aws:codeconnections:*region*:*account-id*:host/*host-id*

TagResource

アクション:codeconnections:TagResource

接続リソースにタグを付けるために必要です。

リソース:arn:aws:codeconnections:*region*:*account-id*:connection/*connection-id*、 arn:aws:codeconnections:*region*:*account-id*:host/*host-id*

UntagResource

アクション:codeconnections:UntagResource

接続リソースからタグを解除するために必要です。

リソース:arn:aws:codeconnections:*region*:*account-id*:connection/*connection-id*、 arn:aws:codeconnections:*region*:*account-id*:host/*host-id*

リポジトリリンクに接続を渡す

同期設定でリポジトリリンクを提供する場合、ユーザーにはリポジトリリンク ARN/リソースに対する codeconnections:PassRepository アクセス許可が必要です。

AWS CodeConnections が接続を渡すために必要なアクセス許可

PassRepository

アクション:codeconnections:PassRepository

リポジトリリンクを同期設定に渡すために必要です。

リソース:arn:aws:codeconnections:*region*:*account-id*:repository-link/*repository-link-id*

このオペレーションでは、次の条件キーもサポートされます。

- codeconnections:PassedToService

条件キーでサポートされる値

Key	有効なアクションプロバイダー
codeconnections:PassedToService	• cloudformation.sync.codeconnections.amazonaws.com

リポジトリリンクでサポートされる条件キー

リポジトリリンクと同期設定リソースの操作は、以下の条件キーでサポートされています。

- codeconnections:Branch

  リクエストで渡されたブランチ名でアクセスをフィルタリングします

条件キーでサポートされるアクション

Key	有効値
codeconnections:Branch	以下のアクションが、この条件キーに対してサポートされています。 • CreateSyncConfiguration • UpdateSyncConfiguration • GetRepositorySyncStatus

接続共有でサポートされているアクセス許可

接続を共有するときは、次の IAM オペレーションが使用されます。

```
codeconnections:GetResourcePolicy
```

AWS CodeConnections が接続を共有するために必要なアクション

GetResourcePolicy

アクション:`codeconnections:GetResourcePolicy`

リソースポリシーに関する情報にアクセスするために必要です。

リソース:`arn:aws:codeconnections:`*region*`:`*account-id*`:connection/`*connection-id*

接続共有の詳細については、「」を参照してください[と接続を共有する AWS アカウント]。

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、 AWS CodeCommit、、または のマネージドポリシーのいずれか AWS CodePipeline が適用されている IAM ユーザーとロールには AWS CodeBuild AWS CodeDeploy、それらのポリシーの意図に沿った接続、通知、および通知ルールに対するアクセス許可があります。例えば、フルアクセスポリシー (AWSCodeCommitFullAccess、AWSCodeBuildAdminAccess、AWSCodeDeployFullAccess、 または AWSCodePipeline_FullAccess) のいずれかを持つ IAM ユーザーまたはロールは、それらのサービスのリソースに対して作成された通知および通知ルールへのフルアクセスを付与されます。

他の IAM ユーザーおよびロールには、 AWS CodeStar Notifications および AWS CodeConnections リソースを作成または変更するアクセス許可がありません。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、必要な指定されたリソースに対して API オペレーションを実行するためのアクセス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。

AWS CodeStar Notifications のアクセス許可と例

次のポリシーステートメントと例は、 AWS CodeStar Notifications の管理に役立ちます。

フルアクセスマネージドポリシーの通知に関連するアクセス許可

AWSCodeCommitFullAccess、AWSCodeBuildAdminAccess、AWSCodeDeployFullAccess、および AWSCodePipeline_FullAccess マネージドポリシーには、デベロッパーツールコンソールの通知へのフルアクセスを許可するために以下のステートメントが含まれています。これらの管理ポリシーのいずれかが適用されたユーザーは、通知の Amazon SNS トピックの作成と管理、トピックに対するユーザーのサブスクライブとサブスクライブ解除、通知ルールのターゲットとして選択するトピックの一覧表示を行うこともできます。

> **Note**
>
> 管理ポリシーでは、条件キー `codestar-notifications:NotificationsForResource` はサービスのリソースタイプに固有の値を持ちます。例えば、CodeCommit のフルアクセスポリシーでは、値は `arn:aws:codecommit:*` です。

```
    {
        "Sid": "CodeStarNotificationsReadWriteAccess",
        "Effect": "Allow",
        "Action": [
            "codestar-notifications:CreateNotificationRule",
            "codestar-notifications:DescribeNotificationRule",
            "codestar-notifications:UpdateNotificationRule",
            "codestar-notifications:DeleteNotificationRule",
            "codestar-notifications:Subscribe",
            "codestar-notifications:Unsubscribe"
        ],
        "Resource": "*",
        "Condition" : {
            "StringLike" : {"codestar-notifications:NotificationsForResource" :
"arn:aws:<vendor-code>:*"}
        }
    },
    {
        "Sid": "CodeStarNotificationsListAccess",
        "Effect": "Allow",
        "Action": [
            "codestar-notifications:ListNotificationRules",
            "codestar-notifications:ListTargets",
            "codestar-notifications:ListTagsforResource",
            "codestar-notifications:ListEventTypes"
```

```
        ],
        "Resource": "*"
    },
    {
        "Sid": "CodeStarNotificationsSNSTopicCreateAccess",
        "Effect": "Allow",
        "Action": [
            "sns:CreateTopic",
            "sns:SetTopicAttributes"
        ],
        "Resource": "arn:aws:sns:*:*:codestar-notifications*"
    },
    {
        "Sid": "SNSTopicListAccess",
        "Effect": "Allow",
        "Action": [
            "sns:ListTopics"
        ],
        "Resource": "*"
    },
    {
        "Sid": "CodeStarNotificationsChatbotAccess",
        "Effect": "Allow",
        "Action": [
            "chatbot:DescribeSlackChannelConfigurations",
            "chatbot:ListMicrosoftTeamsChannelConfigurations"
          ],
       "Resource": "*"
    }
```

読み取り専用マネージドポリシーの通知に関連するアクセス許可

AWSCodeCommitReadOnlyAccess、AWSCodeBuildReadOnlyAccess、AWSCodeDeployReadOnlyAccess、および AWSCodePipeline_ReadOnlyAccess マネージドポリシーには、通知への読み取り専用アクセスを許可するために以下のステートメントが含まれています。例えば、デベロッパーツールコンソールでリソースの通知を表示することはできますが、リソースを作成、管理、サブスクライブすることはできません。

> **Note**
>
> 管理ポリシーでは、条件キー `codestar-notifications:NotificationsForResource` はサービスのリソースタイプに固有の値を持ちます。例えば、CodeCommit のフルアクセスポリシーでは、値は `arn:aws:codecommit:*` です。

```
  {
       "Sid": "CodeStarNotificationsPowerUserAccess",
       "Effect": "Allow",
       "Action": [
           "codestar-notifications:DescribeNotificationRule"
       ],
       "Resource": "*",
       "Condition" : {
           "StringLike" : {"codestar-notifications:NotificationsForResource" :
"arn:aws:<vendor-code>:*"}
       }
   },
   {
       "Sid": "CodeStarNotificationsListAccess",
       "Effect": "Allow",
       "Action": [
           "codestar-notifications:ListNotificationRules",
           "codestar-notifications:ListEventTypes",
           "codestar-notifications:ListTargets"
       ],
       "Resource": "*"
   }
```

その他の管理ポリシーの通知に関連するアクセス許可

AWSCodeCommitPowerUser、AWSCodeBuildDeveloperAccess、および AWSCodeBuildDeveloperAccess 管理ポリシーには、これらの管理ポリシーのいずれかが適用された開発者が、通知を作成、編集、およびサブスクライブできるように、以下のステートメントが含まれています。通知ルールを削除したり、リソースのタグを管理したりすることはできません。

> **Note**
>
> 管理ポリシーでは、条件キー codestar-notifications:NotificationsForResource はサービスのリソースタイプに固有の値を持ちます。例えば、CodeCommit のフルアクセスポリシーでは、値は arn:aws:codecommit:* です。

```
    {
        "Sid": "CodeStarNotificationsReadWriteAccess",
        "Effect": "Allow",
        "Action": [
            "codestar-notifications:CreateNotificationRule",
            "codestar-notifications:DescribeNotificationRule",
            "codestar-notifications:UpdateNotificationRule",
            "codestar-notifications:Subscribe",
            "codestar-notifications:Unsubscribe"
        ],
        "Resource": "*",
        "Condition" : {
            "StringLike" : {"codestar-notifications:NotificationsForResource" :
"arn:aws:<vendor-code>:*"}
        }
    },
    {
        "Sid": "CodeStarNotificationsListAccess",
        "Effect": "Allow",
        "Action": [
            "codestar-notifications:ListNotificationRules",
            "codestar-notifications:ListTargets",
            "codestar-notifications:ListTagsforResource",
            "codestar-notifications:ListEventTypes"
        ],
        "Resource": "*"
    },
    {
        "Sid": "SNSTopicListAccess",
        "Effect": "Allow",
        "Action": [
            "sns:ListTopics"
        ],
        "Resource": "*"
    },
```

```
    {
        "Sid": "CodeStarNotificationsChatbotAccess",
        "Effect": "Allow",
        "Action": [
            "chatbot:DescribeSlackChannelConfigurations",
            "chatbot:ListMicrosoftTeamsChannelConfigurations"
          ],
       "Resource": "*"
    }
```

例: AWS CodeStar Notifications を管理するための管理者レベルのポリシー

この例では、 AWS アカウントの IAM ユーザーに AWS CodeStar Notifications へのフルアクセスを付与して、ユーザーが通知ルールの詳細を確認し、通知ルール、ターゲット、イベントタイプを一覧表示できるようにします。また、通知ルールの追加、更新、および削除をユーザーに許可します。これは、AWSCodeBuildAdminAccess、AWSCodeCommitFullAccess, AWSCodeDeployFullAccess、および AWSCodePipeline_FullAccess マネージドポリシーの一部として含まれる通知アクセス許可に相当する、フルアクセスポリシーです。これらの管理ポリシーと同様に、この種のポリシーステートメントは、 AWS アカウント全体の通知および通知ルールへの完全な管理アクセスを必要とする IAM ユーザー、グループ、またはロールにのみアタッチする必要があります。

> **Note**
>
> このポリシーには、許可として `CreateNotificationRule` が含まれています。このポリシーが IAM ユーザーまたはロールに適用されているユーザーは、そのユーザーがそれらのリソース自体にアクセスできない場合でも、 AWS アカウントで AWS CodeStar Notifications でサポートされているすべてのリソースタイプの通知ルールを作成できます。例えば、このポリシーを持つユーザーは、CodeCommit 自体にアクセスする権限を持たなくても CodeCommit リポジトリの通知ルールを作成できます。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
      {
        "Sid": "AWSCodeStarNotificationsFullAccess",
        "Effect": "Allow",
```

```
        "Action": [
            "codestar-notifications:CreateNotificationRule",
            "codestar-notifications:DeleteNotificationRule",
            "codestar-notifications:DescribeNotificationRule",
            "codestar-notifications:ListNotificationRules",
            "codestar-notifications:UpdateNotificationRule",
            "codestar-notifications:Subscribe",
            "codestar-notifications:Unsubscribe",
            "codestar-notifications:DeleteTarget",
            "codestar-notifications:ListTargets",
            "codestar-notifications:ListTagsforResource",
            "codestar-notifications:TagResource",
            "codestar-notifications:UntagResource"
        ],
        "Resource": "*"
      }
   ]
}
```

例: AWS CodeStar Notifications を使用するためのコントリビューターレベルのポリシー

この例では、通知の作成やサブスクライブなど、 AWS CodeStar Notifications day-to-day使用状況へのアクセスを許可しますが、通知ルールやターゲットの削除など、より破壊的なアクションへのアクセスは許可しません。これは、AWSCodeBuildDeveloperAccess、AWSCodeDeployDeveloperAccess、および AWSCodeCommitPowerUser 管理ポリシーで提供されるアクセスに相当します。

> **Note**
>
> このポリシーには、許可として `CreateNotificationRule` が含まれています。このポリシーが IAM ユーザーまたはロールに適用されているユーザーは、そのユーザーがそれらのリソース自体にアクセスできない場合でも、 AWS アカウントで AWS CodeStar Notifications でサポートされているすべてのリソースタイプの通知ルールを作成できます。例えば、このポリシーを持つユーザーは、CodeCommit 自体にアクセスする権限を持たなくても CodeCommit リポジトリの通知ルールを作成できます。

```
{
    "Version": "2012-10-17",
    "Sid": "AWSCodeStarNotificationsPowerUserAccess",
```

```
        "Effect": "Allow",
        "Action": [
            "codestar-notifications:CreateNotificationRule",
            "codestar-notifications:DescribeNotificationRule",
            "codestar-notifications:ListNotificationRules",
            "codestar-notifications:UpdateNotificationRule",
            "codestar-notifications:Subscribe",
            "codestar-notifications:Unsubscribe",
            "codestar-notifications:ListTargets",
            "codestar-notifications:ListTagsforResource"
        ],
        "Resource": "*"
        }
    ]
}
```

例: AWS CodeStar Notifications を使用するためのread-only-levelポリシー

次の例では、アカウントの IAM ユーザーに対して、 AWS アカウントで通知ルール、ターゲット、およびイベントタイプへの読み取り専用アクセスを付与します。この例は、これらの項目の表示を許可するポリシーの作成方法を示しています。これは、AWSCodeBuildReadOnlyAccess、AWSCodeCommitReadOnly、および AWSCodePipeline_ReadOnlyAccess 管理ポリシーの一部として含まれるアクセス許可に相当します。

JSON

```
{
    "Version":"2012-10-17",
    "Id": "CodeNotificationforReadOnly",
    "Statement": [
        {
            "Sid": "ReadsAccess",
            "Effect": "Allow",
            "Action": [
                "codestar-notifications:DescribeNotificationRule",
                "codestar-notifications:ListNotificationRules",
                "codestar-notifications:ListTargets",
                "codestar-notifications:ListEventTypes"
            ],
            "Resource": "*"
        }
```

```
    ]
}
```

のアクセス許可と例 AWS CodeConnections

以下のポリシーステートメントと例は、 AWS CodeConnectionsの管理に役立ちます。

これらの JSON ポリシードキュメント例を使用して IAM の ID 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。

例: CLI AWS CodeConnections で を作成し、コンソールで表示するためのポリシー

AWS CLI または SDK を使用して接続を表示、作成、タグ付け、または削除するように指定されたロールまたはユーザーには、以下に制限されたアクセス許可が必要です。

> **Note**
>
> 次のアクセス許可のみでは、コンソールでの接続を完了することはできません。次のセクションでアクセス許可を追加する必要があります。

コンソールを使用して、使用可能な接続の一覧を表示し、タグを表示し、接続を使用するには、次のポリシーを使用します。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
      {
        "Sid": "ConnectionsFullAccess",
        "Effect": "Allow",
        "Action": [
            "codeconnections:CreateConnection",
            "codeconnections:DeleteConnection",
            "codeconnections:UseConnection",
            "codeconnections:GetConnection",
            "codeconnections:ListConnections",
            "codeconnections:TagResource",
            "codeconnections:ListTagsForResource",
```

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

例: コンソール AWS CodeConnections で を作成するためのポリシー

コンソールで接続を管理するように指定されたロールまたはユーザーは、コンソールで接続を完了し、インストールを作成するために必要なアクセス許可を持っている必要があります。これには、プロバイダーへのハンドシェイクの許可と、使用する接続用のインストールの作成が含まれます。UseConnection もまたコンソールで接続を使用するために追加する必要があります。コンソールで接続を表示、使用、作成、タグ付け、または削除するには、次のポリシーを使用します。

> **Note**
>
> 2024 年 7 月 1 日以降、コンソールはリソース ARN codeconnectionsに との接続を作成します。両方のサービスプレフィックスを持つリソースは、コンソールに引き続き表示されます。

> **Note**
>
> コンソールを使用して作成されたリソースの場合、次の例に示すように、ポリシーステートメントアクションにはサービスプレフィックスcodestar-connectionsとして を含める必要があります。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "codestar-connections:CreateConnection",
```

```
                "codestar-connections:DeleteConnection",
                "codestar-connections:GetConnection",
                "codestar-connections:ListConnections",
                "codestar-connections:GetInstallationUrl",
                "codestar-connections:GetIndividualAccessToken",
                "codestar-connections:ListInstallationTargets",
                "codestar-connections:StartOAuthHandshake",
                "codestar-connections:UpdateConnectionInstallation",
                "codestar-connections:UseConnection",
                "codestar-connections:TagResource",
                "codestar-connections:ListTagsForResource",
                "codestar-connections:UntagResource"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

例: を管理するための管理者レベルのポリシー AWS CodeConnections

この例では、 AWS アカウントの IAM ユーザーに CodeConnections へのフルアクセスを付与して、ユーザーが接続を追加、更新、削除できるようにします。これはフルアクセスポリシーであり、AWSCodePipeline_FullAccess 管理ポリシーと同等です。その管理ポリシーと同様に、この種のポリシーステートメントは、 AWS アカウント全体の接続への完全な管理アクセスを必要とする IAM ユーザー、グループ、またはロールにのみアタッチする必要があります。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
      {
        "Sid": "ConnectionsFullAccess",
        "Effect": "Allow",
        "Action": [
            "codeconnections:CreateConnection",
            "codeconnections:DeleteConnection",
            "codeconnections:UseConnection",
            "codeconnections:GetConnection",
```

```
            "codeconnections:ListConnections",
            "codeconnections:ListInstallationTargets",
            "codeconnections:GetInstallationUrl",
            "codeconnections:StartOAuthHandshake",
            "codeconnections:UpdateConnectionInstallation",
            "codeconnections:GetIndividualAccessToken",
            "codeconnections:TagResource",
            "codeconnections:ListTagsForResource",
            "codeconnections:UntagResource"
        ],
        "Resource": "*"
     }
   ]
}
```

例: を使用するための寄稿者レベルのポリシー AWS CodeConnections

この例では、接続の詳細の作成や表示など、CodeConnections のday-to-day使用状況へのアクセスを許可しますが、接続の削除など、より破壊的なアクションへのアクセスは許可しません。

JSON

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

```
    ]
}
```

例: を使用するためのread-only-levelポリシー AWS CodeConnections

この例では、アカウントの IAM ユーザーに、アカウントの接続への読み取り専用アクセスを付与します AWS 。この例は、これらの項目の表示を許可するポリシーの作成方法を示しています。

JSON

```
{
    "Version":"2012-10-17",
    "Id": "ConnectionsforReadOnly",
    "Statement": [
        {
            "Sid": "ReadsAPIAccess",
            "Effect": "Allow",
            "Action": [
            "codeconnections:GetConnection",
            "codeconnections:ListConnections",
            "codeconnections:ListInstallationTargets",
            "codeconnections:GetInstallationUrl",
            "codeconnections:ListTagsForResource"
            ],
            "Resource": "*"
        }
    ]
}
```

例: VpcId コンテキストキーを使用してホスト VPC アクセス許可を制限する

次の例では、お客様は VpcId コンテキストキーを使用して、ホストの作成または管理を、指定された VPC を持つホストに制限できます。

JSON

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

```
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "codeconnections:CreateHost",
                "codeconnections:UpdateHost"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "codeconnections:VpcId": "vpc-EXAMPLE"
                }
            }
        }
    ]
}
```

タグを使用して AWS CodeConnections リソースへのアクセスを制御する

タグは、リソースにアタッチしたり、タグ付けをサポートするサービスへのリクエストに渡したりすることができます。In AWS CodeConnections では、リソースにタグを付けることができ、一部のアクションにはタグを含めることができます。IAM ポリシーを作成するときに、タグ条件キーを使用して以下をコントロールできます。

- どのユーザーがパイプラインリソースに対してアクションを実行できるか (リソースに既に付けられているタグに基づいて)。
- どのタグをアクションのリクエストで渡すことができるか。
- リクエストで特定のタグキーを使用できるかどうか。

次の例は、CodeConnections ユーザーのポリシー AWS でタグ条件を指定する方法を示しています。

Example 1: リクエストのタグに基づいてアクションを許可する

次のポリシーは、CodeConnections で AWS 接続を作成するアクセス許可をユーザーに付与します。

これを行うには、リクエストに指定されているタグ `Project` の値が `ProjectA` である場合に、`CreateConnection` アクションと `TagResource` アクションを許可します。(この

aws:RequestTag 条件キーを使用して、IAM リクエストで渡すことができるタグをコントロールします)。aws:TagKeys 条件は、タグキーの大文字と小文字を区別します。

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "codeconnections:CreateConnection",
        "codeconnections:TagResource"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:RequestTag/Project": "ProjectA"
        },
        "ForAllValues:StringEquals": {
          "aws:TagKeys": ["Project"]
        }
      }
    }
  ]
}
```

Example 2: リソースタグに基づいてアクションを制限する

次のポリシーは、 AWS CodeConnections のリソースに対してアクションを実行し、その情報を取得するアクセス許可をユーザーに付与します。

これを行うには、パイプラインに含まれているタグ Project の値が ProjectA である場合に、特定のアクションを許可します。(この aws:RequestTag 条件キーを使用して、IAM リクエストで渡すことができるタグをコントロールします)。aws:TagKeys 条件は、タグキーの大文字と小文字を区別します。

JSON

```
{
```

```
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "codeconnections:CreateConnection",
        "codeconnections:DeleteConnection",
        "codeconnections:ListConnections"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/Project": "ProjectA"
        },
        "ForAllValues:StringEquals": {
          "aws:TagKeys": ["Project"]
        }
      }
    }
  ]
}
```

コンソールでの通知と接続の使用

この通知エクスペリエンスは、CodeBuild、CodeCommit、CodeDeploy、CodePipeline の各コンソールの他、[設定] ナビゲーションバー自体のデベロッパーツールコンソールにも組み込まれています。コンソールで通知にアクセスするには、それらのサービスにいずれかの管理ポリシーを適用するか、最小限のアクセス許可のセットが必要です。これらのアクセス許可により、 AWS アカウントの AWS CodeStar Notifications および AWS CodeConnections リソースの詳細を一覧表示および表示できます。最小限必要な許可よりも厳しく制限されたアイデンティティベースポリシーを作成すると、そのポリシーを添付したエンティティ (IAM ユーザーまたはロール) に対してコンソールが意図したとおりに機能しません。これらのコンソールへのアクセスの許可 AWS CodeBuild AWS CodeCommit AWS CodeDeploy、およびそれらのコンソールへのアクセスの許可の詳細については AWS CodePipeline、以下のトピックを参照してください。

- CodeBuild: CodeBuild のアイデンティティベースのポリシーの使用
- CodeCommit: CodeCommit のアイデンティティベースのポリシーの使用
- AWS CodeDeploy: の ID とアクセスの管理 AWS CodeDeploy
- CodePipeline: IAM ポリシーを使用したアクセスコントロール

AWS CodeStar Notifications には AWS 管理ポリシーはありません。通知機能へのアクセスを提供するには、上記のいずれかのサービスに対する管理ポリシーの 1 つを適用するか、ユーザーまたはエンティティに付与するアクセス許可のレベルでポリシーを作成してから、これらのアクセス許可が必要なユーザー、グループ、またはロールにそれらのポリシーをアタッチする必要があります。詳細については、次の例を参照してください。

- 例: AWS CodeStar Notifications を管理するための管理者レベルのポリシー
- 例: AWS CodeStar Notifications を使用するためのコントリビューターレベルのポリシー
- 例: AWS CodeStar Notifications を使用するためのread-only-levelポリシー.

AWS CodeConnections には AWS 管理ポリシーはありません。接続を完了するためのアクセス許可で詳しく説明している許可など、アクセスの許可や許可の組み合わせを使用します。

詳細については次を参照してください:

- 例: を管理するための管理者レベルのポリシー AWS CodeConnections
- 例: を使用するための寄稿者レベルのポリシー AWS CodeConnections
- 例: を使用するためのread-only-levelポリシー AWS CodeConnections

AWS CLI または AWS API のみを呼び出すユーザーには、コンソールの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 Notifications と AWS CodeConnections 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、通知と 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

- 管理者として通知へのアクセスを他のユーザーに許可したい
- Amazon SNS トピックを作成して通知ルールのターゲットとして追加したが、イベントに関する E メールが届かない
- AWS アカウント以外のユーザーに my AWS CodeStar Notifications および AWS CodeConnections リソースへのアクセスを許可したい

管理者として通知へのアクセスを他のユーザーに許可したい

他のユーザーが AWS CodeStar Notifications と AWS CodeConnections にアクセスできるようにするには、アクセスが必要なユーザーまたはアプリケーションにアクセス許可を付与する必要があります。 AWS IAM アイデンティティセンター を使用してユーザーとアプリケーションを管理する場合は、アクセスレベルを定義するアクセス許可セットをユーザーまたはグループに割り当てます。アクセス許可セットは、ユーザーまたはアプリケーションに関連付けられている IAM ロールに自動的に IAM ポリシーを作成して割り当てます。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「アクセス許可セット」を参照してください。

IAM アイデンティティセンターを使用していない場合は、アクセスを必要としているユーザーまたはアプリケーションの IAM エンティティ (ユーザーまたはロール) を作成する必要があります。次に、 AWS CodeStar Notifications と AWS CodeConnections の適切なアクセス許可を付与するポリシーをエンティティにアタッチする必要があります。アクセス許可が付与されたら、ユーザーまたはアプリケーション開発者に認証情報を提供します。これらの認証情報を使用して AWSにアクセスします。IAM ユーザー、グループ、ポリシー、アクセス許可の作成の詳細については、「IAM ユーザーガイド」の「IAM アイデンティティ」と「IAM のポリシーとアクセス許可」を参照してください。

AWS CodeStar Notifications 固有の情報については、「」を参照してくださいAWS CodeStar Notifications のアクセス許可と例。

Amazon SNS トピックを作成して通知ルールのターゲットとして追加したが、イベントに関する E メールが届かない

イベントに関する通知を受信するには、通知ルールのターゲットとして有効な Amazon SNS トピックがサブスクライブされていること、および E メールアドレスが Amazon SNS トピックにサブスクライブされていることが必要です。Amazon SNS トピックの問題のトラブルシューティングを行うには、以下を確認します。

- Amazon SNS トピックが通知ルールと同じ AWS リージョンにあることを確認します。
- E メールエイリアスが正しいトピックにサブスクライブされていること、およびサブスクリプションを確認済みであることを確認します。詳細については、「Amazon SNS トピックにエンドポイントをサブスクライブする」を参照してください。
- トピックポリシーが変更され、 AWS CodeStar Notifications がそのトピックに通知をプッシュできることを確認します。トピックポリシーには、次のようなステートメントを含める必要があります。

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

詳細については、「セットアップ」を参照してください。

AWS アカウント以外のユーザーに my AWS CodeStar Notifications および AWS CodeConnections 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 Notifications と AWS CodeConnections 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、「」を参照してくださいデベロッパーツールコンソールの機能と IAM との連携方法。
- 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「サードパーティーが所有する へのアクセスを提供する AWS アカウント」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。

AWS CodeStar Notifications のサービスにリンクされたロールの使用

AWS CodeStar Notifications は AWS Identity and Access Management 、(IAM) サービスにリンクされたロールを使用します。サービスにリンクされたロールは、 AWS CodeStar Notifications に直接リンクされた一意のタイプの IAM ロールです。サービスリンクロールは AWS CodeStar Notifications によって事前に定義されており、サービスがユーザーに代わって AWS の他のサービスを呼び出すために必要なすべての許可が含まれています。このロールは、通知ルールを初めて作成したときに自動的に作成されます。ユーザーがロールを作成する必要はありません。

サービスにリンクされたロールを使用すると、手動でアクセス許可を追加する必要がないため、AWS CodeStar Notifications の設定が簡単になります。 AWS CodeStar Notifications は、サービスにリンクされたロールのアクセス許可を定義し、特に定義されている場合を除き、 AWS CodeStar Notifications のみがそのロールを引き受けることができます。定義される許可は信頼ポリシーと許可ポリシーに含まれており、その許可ポリシーを他の IAM エンティティにアタッチすることはできません。

サービスにリンクされたロールを削除するには、まず関連するリソースを削除する必要があります。これにより、リソースへのアクセス許可が誤って削除されないため、 AWS CodeStar Notifications リソースが保護されます。

サービスにリンクされたロールをサポートしているその他のサービスの詳細については、「IAM と連携するAWS のサービス」を参照してください。

AWS CodeStar Notifications のサービスにリンクされたロールのアクセス許可

AWS CodeStar Notifications は、AWSServiceRoleForCodeStarNotifications サービスにリンクされたロールを使用して、ツールチェーンで発生するイベントに関する情報を取得し、指定したターゲットに通知を送信します。

AWSServiceRoleForCodeStarNotifications サービスリンクロールは、以下のサービスを信頼してロールを引き受けます。

- `codestar-notifications.amazonaws.com`

ロールのアクセス許可ポリシーにより、 AWS CodeStar Notifications は指定されたリソースに対して次のアクションを実行できます。

- アクション: PutRule。対象リソース: CloudWatch Event rules that are named awscodestar-notifications-*
- アクション: CloudWatch Event rules that are named awscodestar-notifications-* 上で DescribeRule
- アクション: PutTargets。対象リソース: CloudWatch Event rules that are named awscodestar-notifications-*
- アクション: CreateTopic (create Amazon SNS topics for use with AWS CodeStar Notifications with the prefix CodeStarNotifications- が対象)
- アクション: GetCommentsForPullRequests。対象リソース: all comments on all pull requests in all CodeCommit repositories in the AWS account
- アクション: all comments on all commits in all CodeCommit repositories in the AWS account 上で GetCommentsForComparedCommit
- アクション: all commits in all CodeCommit repositories in the AWS account 上で GetDifferences
- アクション: all comments on all commits in all CodeCommit repositories in the AWS account 上で GetCommentsForComparedCommit
- アクション: all commits in all CodeCommit repositories in the AWS account 上で GetDifferences
- アクション: all AWS Chatbot clients in the AWS account 上で DescribeSlackChannelConfigurations
- アクション: all AWS Chatbot clients in the AWS account 上で UpdateSlackChannelConfiguration
- アクション: all actions in all pipelines in the AWS account 上で ListActionExecutions
- アクション: GetFile。対象リソース: all files in all CodeCommit repositories in the AWS account unless otherwise tagged

これらのアクションは、AWSServiceRoleForCodeStarNotifications サービスにリンクされたロールのポリシーステートメントで確認できます。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Action": [
                "events:PutTargets",
                "events:PutRule",
                "events:DescribeRule"
            ],
            "Resource": "arn:aws:events:*:*:rule/awscodestarnotifications-*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "sns:CreateTopic"
            ],
            "Resource": "arn:aws:sns:*:*:CodeStarNotifications-*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "codecommit:GetCommentsForPullRequest",
                "codecommit:GetCommentsForComparedCommit",
                "codecommit:GetDifferences",
                "chatbot:DescribeSlackChannelConfigurations",
                "chatbot:UpdateSlackChannelConfiguration",
                "codepipeline:ListActionExecutions"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "codecommit:GetFile"
            ],
            "Resource": "*",
            "Condition": {
                "StringNotEquals": {
                    "aws:ResourceTag/ExcludeFileContentFromNotifications": "true"
                }
            },
```

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

サービスリンクロールの作成、編集、削除を IAM エンティティ (ユーザー、グループ、ロールなど) に許可するにはアクセス許可を設定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「サービスリンクロールの許可」を参照してください。

AWS CodeStar Notifications のサービスにリンクされたロールの作成

サービスリンクロールを手動で作成する必要はありません。開発者ツールコンソールまたは AWS CLI または SDKs の CreateNotificationRule API を使用して、通知ルールを作成できます。API を直接呼び出すこともできます。使用する方法にかかわらず、サービスにリンクされたロールが作成されます。

このサービスリンクロールを削除した後で再度作成する必要が生じた場合は同じ方法でアカウントにロールを再作成できます。開発者ツールコンソールまたは AWS CLI または SDKs の CreateNotificationRule API を使用して、通知ルールを作成できます。API を直接呼び出すこともできます。使用する方法にかかわらず、サービスにリンクされたロールが作成されます。

AWS CodeStar Notifications のサービスにリンクされたロールの編集

サービスにリンクされたロールを作成すると、多くのエンティティによってロールが参照される可能性があるため、名前を変更することはできません。ただし、IAM を使用してロールの説明を編集することはできます。詳細については、「IAM ユーザーガイド」の「サービスリンクロールの編集」を参照してください。

AWS CodeStar Notifications のサービスにリンクされたロールの削除

サービスにリンクされたロールが必要な機能またはサービスが不要になった場合には、そのロールを削除することをお勧めします。そうすることで、使用していないエンティティがアクティブにモニタリングされたり、メンテナンスされたりすることがなくなります。削除する前に、サービスにリンクされたロールのリソースをクリーンアップする必要があります。 AWS CodeStar Notifications の場合、これは AWS アカウントでサービスロールを使用するすべての通知ルールを削除することを意味します。

> **Note**
>
> リソースを削除しようとしたときに AWS CodeStar Notifications サービスがロールを使用している場合は、削除が失敗する可能性があります。失敗した場合は数分待ってから操作を再試行してください。

AWSServiceRoleFor AWS CodeStar Notificationsで使用される CodeStar Notifications リソースを削除するには AWSServiceRoleForCodeStarNotifications

1. https://console.aws.amazon.com/codesuite/settings/notifications で AWS デベロッパーツールコンソールを開きます。

   > **Note**
   >
   > 通知ルールは、作成された AWS リージョンに適用されます。複数の AWS リージョンに通知ルールがある場合は、リージョンセレクタを使用して を変更します AWS リージョン。

2. リストに表示されるすべての通知ルールを選択し、 [Delete (削除)] を選択します。
3. 通知ルールを作成したすべての AWS リージョンで、これらのステップを繰り返します。

IAM を使用して、サービスにリンクされたロールを削除するには

IAM コンソール AWS CLI、または AWS Identity and Access Management API を使用して、AWSServiceRoleForCodeStarNotifications サービスにリンクされたロールを削除します。詳細については、「IAM ユーザーガイド」の「サービスリンクロールの削除」を参照してください。

AWS CodeStar Notifications サービスにリンクされたロールでサポートされているリージョン

AWS CodeStar Notifications は、サービスが利用可能なすべての AWS リージョンでサービスにリンクされたロールの使用をサポートしています。詳細については、「AWS のリージョンとエンドポイント」および「AWS CodeStar Notifications」を参照してください。

のサービスにリンクされたロールの使用 AWS CodeConnections

AWS CodeConnections は AWS Identity and Access Management (IAM) サービスにリンクされたロールを使用します。サービスにリンクされたロールは、直接リンクされた一意のタイプの IAM

ロールです AWS CodeConnections。サービスにリンクされたロールは によって事前定義 AWS CodeConnections されており、サービスがユーザーに代わって他の AWS サービスを呼び出すために必要なすべてのアクセス許可が含まれています。このロールは、接続を初めて作成するときにお客様用に作成されます。ユーザーがロールを作成する必要はありません。

サービスにリンクされたロールを使用すると、アクセス許可を手動で追加する必要がなくなるため、の設定 AWS CodeConnections が簡単になります。 は、サービスにリンクされたロールのアクセス許可 AWS CodeConnections を定義し、特に定義されている場合を除き、 のみがそのロールを引き受け AWS CodeConnections ることができます。定義される許可は信頼ポリシーと許可ポリシーに含まれており、その許可ポリシーを他の IAM エンティティにアタッチすることはできません。

サービスにリンクされたロールを削除するには、まず関連するリソースを削除する必要があります。これにより、 AWS CodeConnections リソースへのアクセス許可が誤って削除されないため、リソースが保護されます。

サービスにリンクされたロールをサポートしているその他のサービスの詳細については、「IAM と連携するAWS のサービス」を参照してください。

> **Note**
>
> 新しいサービスプレフィックスで作成されたリソースのアクションcodeconnectionsを使用できます。新しいサービスプレフィックスでリソースを作成すると、リソース ARN codeconnectionsで が使用されます。codestar-connections サービスプレフィックスのアクションとリソースは引き続き使用できます。IAM ポリシーでリソースを指定する場合、サービスプレフィックスはリソースのプレフィックスと一致する必要があります。

のサービスにリンクされたロールのアクセス許可 AWS CodeConnections

AWS CodeConnections は、AWSServiceRoleForGitSync サービスにリンクされたロールを使用して、接続された Git ベースのリポジトリとの Git 同期を使用します。

サービスにリンクされたロール AWSServiceRoleForGitSync は、次のサービスを信頼してそのロールを引き受けます。

- `repository.sync.codeconnections.amazonaws.com`

AWSGitSyncServiceRolePolicy という名前のロールアクセス許可ポリシーにより AWS CodeConnections 、 は指定されたリソースに対して次のアクションを実行できます。

- アクション: 外部の Git ベースのリポジトリへの接続を作成し、それらのレポジトリで Git 同期を使用できるようにするアクセス許可を、ユーザーに付与します。

サービスリンクロールの作成、編集、削除を IAM エンティティ (ユーザー、グループ、ロールなど) に許可するにはアクセス許可を設定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「サービスリンクロールの許可」を参照してください。

のサービスにリンクされたロールの作成 AWS CodeConnections

サービスリンクロールを手動で作成する必要はありません。ロールは、CreateRepositoryLink API を使用して Git 同期プロジェクトのリソースを作成するときに作成します。

このサービスリンクロールを削除した後で再度作成する必要が生じた場合は同じ方法でアカウントにロールを再作成できます。

のサービスにリンクされたロールの編集 AWS CodeConnections

サービスにリンクされたロールを作成すると、多くのエンティティによってロールが参照される可能性があるため、名前を変更することはできません。ただし、IAM を使用してロールの説明を編集することはできます。詳細については、「IAM ユーザーガイド」の「サービスリンクロールの編集」を参照してください。

のサービスにリンクされたロールの削除 AWS CodeConnections

サービスにリンクされたロールが必要な機能またはサービスが不要になった場合には、そのロールを削除することをお勧めします。そうすることで、使用していないエンティティがアクティブにモニタリングされたり、メンテナンスされたりすることがなくなります。削除する前に、サービスにリンクされたロールのリソースをクリーンアップする必要があります。つまり、 AWS アカウントで サービスロールを使用するすべての接続を削除します。

> **Note**
>
> リソースを削除しようとしたときに AWS CodeConnections サービスがロールを使用している場合、削除が失敗する可能性があります。失敗した場合は数分待ってから操作を再試行してください。

AWSServiceRoleForGitSync で使用される AWS CodeConnections リソースを削除するには

1. 開発者ツールコンソールを開き、[設定] を選択します。

2. リストに表示されるすべての接続を選択し、[削除] を選択します。
3. 接続を作成したすべての AWS リージョンで、これらのステップを繰り返します。

IAM を使用して、サービスにリンクされたロールを削除するには

IAM コンソール AWS CLI、または AWS Identity and Access Management API を使用して、AWSServiceRoleForGitSync サービスにリンクされたロールを削除します。詳細については、「IAM ユーザーガイド」の「サービスリンクロールの削除」を参照してください。

AWS CodeConnections サービスにリンクされたロールでサポートされているリージョン

AWS CodeConnections は、サービスが利用可能なすべての AWS リージョンでサービスにリンクされたロールの使用をサポートします。詳細については、「AWS リージョンとエンドポイント」を参照してください。

AWS の 管理ポリシー AWS CodeConnections

AWS 管理ポリシーは、 によって作成および管理されるスタンドアロンポリシーです AWS。 AWS 管理ポリシーは、ユーザー、グループ、ロールにアクセス許可の割り当てを開始できるように、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ように設計されています。

AWS 管理ポリシーは、すべての AWS お客様が使用できるため、特定のユースケースに対して最小特権のアクセス許可を付与しない場合があることに注意してください。ユースケースに固有のカスタマー管理ポリシーを定義して、アクセス許可を絞り込むことをお勧めします。

AWS 管理ポリシーで定義されているアクセス許可は変更できません。が AWS マネージドポリシーで定義されたアクセス許可 AWS を更新すると、ポリシーがアタッチされているすべてのプリンシパル ID (ユーザー、グループ、ロール) に影響します。 AWS は、新しい が起動されるか、新しい API オペレーション AWS のサービス が既存のサービスで使用できるようになったときに、 AWS マネージドポリシーを更新する可能性が最も高くなります。

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」を参照してください。

> **Note**
>
> 新しいサービスプレフィックスで作成されたリソースのアクションcodeconnectionsを使用できます。新しいサービスプレフィックスでリソースを作成すると、リソース ARN

codeconnectionsで が使用されます。codestar-connections サービスプレフィックスのアクションとリソースは引き続き使用できます。IAM ポリシーでリソースを指定する場合、サービスプレフィックスはリソースのプレフィックスと一致する必要があります。

AWS マネージドポリシー: AWSGitSyncServiceRolePolicy

お客様の IAM エンティティに、AWSGitSyncServiceRolePolicy をアタッチすることはできません。このポリシーは、 がユーザーに代わってアクションを実行できるようにするサービスにリンクされたロール AWS CodeConnections にアタッチされます。詳細については、「のサービスにリンクされたロールの使用 AWS CodeConnections」を参照してください。

このポリシーにより、お客様は Git ベースのリポジトリにアクセスして接続に使用することができます。お客様は CreateRepositoryLink API を使用した後に、これらのリソースにアクセスします。

アクセス許可の詳細

このポリシーには、以下のアクセス許可が含まれています。

- codeconnections – ユーザーが外部 Git ベースのリポジトリへの接続を作成できるようにするアクセス許可を付与します。

JSON

```
{
 "Version":"2012-10-17",
 "Statement": [
  {
   "Sid": "AccessGitRepos",
   "Effect": "Allow",
   "Action": [
```

```
      "codestar-connections:UseConnection",
      "codeconnections:UseConnection"
    ],
    "Resource": [
      "arn:aws:codestar-connections:*:*:connection/*",
      "arn:aws:codeconnections:*:*:connection/*"
    ],
    "Condition": {
      "StringEquals": {
        "aws:ResourceAccount": "${aws:PrincipalAccount}"
      }
    }
   }
  ]
}
```

AWS CodeConnections 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 AWS CodeConnections してからの の AWS 管理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アラートについては、 AWS CodeConnections ドキュメント履歴ページの RSS フィードにサブスクライブしてください。

変更	説明	日付
AWSGitSyncServiceRolePolicy – 更新されたポリシー	AWS CodeStar Connections サービス名が に変更されました AWS CodeConnections。両方のサービスプレフィックスを含む ARNs を持つリソースのポリシーを更新しました。	2024 年 4 月 26 日
AWSGitSyncServiceRolePolicy – 新しいポリシー	AWS CodeStar Connections にポリシーが追加されました。 接続ユーザーが接続された Git ベースのリポジトリと Git 同期を使用できるようにするアクセス許可を付与します。	2023 年 11 月 26 日

変更	説明	日付
AWS CodeConnections が変更の追跡を開始しました	AWS CodeConnections は、AWS 管理ポリシーの変更の追跡を開始しました。	2023 年 11 月 26 日

AWS CodeStar Notifications と AWS CodeConnections のコンプライアンス検証

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の対象となる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。

AWS CodeStar Notifications と AWS CodeConnections を使用する際のお客様のコンプライアンス責任は、お客様のデータの機密性、貴社のコンプライアンス目的、適用される法律および規制によって決まります。 AWS では、コンプライアンスに役立つ以下のリソースを提供しています。

- セキュリティとコンプライアンスのクイックスタートガイド – これらのデプロイガイドでは、アーキテクチャ上の考慮事項について説明し、セキュリティとコンプライアンスに重点を置いたベースライン環境をデプロイする手順について説明します AWS。
- AWS コンプライアンスリソース – このワークブックとガイドのコレクションは、お客様の業界や地域に適用される場合があります。
- AWS Config – この AWS サービスは、リソース設定が内部プラクティス、業界ガイドライン、および規制にどの程度準拠しているかを評価します。
- AWS Security Hub CSPM – この AWS サービスは、 内のセキュリティ状態を包括的に把握 AWS し、セキュリティ業界標準とベストプラクティスへの準拠を確認するのに役立ちます。

AWS CodeStar Notifications と AWS CodeConnections の耐障害性

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、高冗長ネットワークで接続された、物理的に分離および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。

- 通知ルールは、作成された AWS リージョン に固有です。複数の に通知ルールがある場合は AWS リージョン、リージョンセレクタを使用して、それぞれの通知ルールを確認します AWS リージョン。
- AWS CodeStar Notifications は、通知ルールのターゲットとして Amazon Simple Notification Service (Amazon SNS) トピックに依存しています。Amazon SNS トピックと通知ルールのターゲットに関する情報は、通知ルールを設定した リージョンと異なる AWS リージョンに保存される場合があります。

AWS CodeStar Notifications と AWS CodeConnections のインフラストラクチャセキュリティ

マネージドサービスの機能として、 AWS CodeStar Notifications と AWS CodeConnections は、ホワイトペーパー「Amazon Web Services: セキュリティプロセスの概要」で説明されている AWS グローバルネットワークセキュリティ手順によって保護されています。

AWS 公開された API コールを使用して、ネットワーク経由で AWS CodeStar Notifications と AWS CodeConnections にアクセスします。クライアントで Transport Layer Security (TLS) 1.0 以降がサポートされている必要があります。また、Ephemeral Diffie-Hellman (DHE) や Elliptic Curve Ephemeral Diffie-Hellman (ECDHE) などの Perfect Forward Secrecy (PFS) を使用した暗号スイートもクライアントでサポートされている必要があります。最新のシステムは、ほとんどの場合これらのモードをサポートしています。

リクエストは、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の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。

リージョン間の AWS CodeConnections リソース間のトラフィック

接続機能を使用してリソースの接続を有効にする場合、基盤となるサービス AWS リージョン を使用している AWS リージョン の外部に、リソースが作成されたリージョン以外のリージョンでその

ようなリソースへの接続を提供する目的でのみ、そのような接続リソースに関連する情報を保存および処理することに同意し、指示します。

詳細については、「グローバルリソース in AWS CodeConnections」を参照してください。

> **Note**
>
> 接続機能を使用して、先立って有効にする必要のないリージョンでリソースへの接続を有効にした場合、情報は前述のトピックで詳しく説明したとおりに保存および処理されます。欧州 (ミラノ) リージョンなど、先立って有効にする必要があるリージョンで確立した接続については、当リージョンのその接続に関する情報のみが保存および処理されます。

接続の名前変更 - 変更の概要

デベロッパーツールコンソールの接続機能を使用すると、 AWS リソースをサードパーティーのソースリポジトリに接続できます。2024 年 3 月 29 日、 AWS CodeStar Connections の名前が AWS CodeConnections に変更されました。以下のセクションでは、名前の変更に伴って変更された機能のさまざまな部分と、リソースが正常に機能し続けるために実行する必要があるアクションについて説明します。

これはすべてを網羅したリストではないことに注意してください。製品の他の部分も変更されましたが、これらの更新が最も関連性があります。

> **Note**
>
> 新しいサービスプレフィックスで作成されたリソースのアクションcodeconnectionsを使用できます。新しいサービスプレフィックスでリソースを作成すると、リソース ARN codeconnectionsで が使用されます。codestar-connections サービスプレフィックスのアクションとリソースは引き続き使用できます。IAM ポリシーでリソースを指定する場合、サービスプレフィックスはリソースのプレフィックスと一致する必要があります。

> **Note**
>
> 2024 年 7 月 1 日以降、コンソールはリソース ARN codeconnectionsに との接続を作成します。両方のサービスプレフィックスを持つリソースは、コンソールに引き続き表示されます。

名前が変更されたサービスプレフィックス

Connections APIs、名前が変更されたサービスプレフィックス を使用しますcodeconnections。

CLI コマンドで新しいプレフィックスを使用するには、 のバージョン 2 をダウンロードします AWS CLI。以下は、更新されたプレフィックスを持つコマンドの例です。

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

IAM で名前を変更したアクション

IAM のアクションでは、次の例に示すように、新しいプレフィックスを使用します。

```
codeconnections:CreateConnection
codeconnections:DeleteConnection
codeconnections:GetConnection
codeconnections:ListConnections
```

新しいリソース ARN

作成された Connections リソースには新しい ARN があります。

```
arn:aws:codeconnections:us-west-2:account-ID:connection/*
```

影響を受けるサービスロールポリシー

以下のサービスの場合、サービスロールポリシーはポリシーステートメントで新しいプレフィックスを使用します。既存のサービスロールポリシーを更新して新しいアクセス許可を使用することもできますが、古いプレフィックスで作成されたポリシーは引き続きサポートされます。

- CodePipeline カスタマー管理サービスロールポリシー
- AWS CodeStar サービスロール`AWSCodeStarServiceRole`ポリシー

新しい CloudFormation リソース

接続 CloudFormation にリソースを使用するには、新しいリソースを使用できます。既存のリソースは引き続きサポートされます。

- 新しいAWS CloudFormationリソースの名前は AWS::CodeConnections::Connection です。CloudFormation ユーザーガイドのAWS::CodeConnections::Connection」を参照してください。
- 既存の AWS::CodeStarConnections::Connection リソースは引き続きサポートされます。CloudFormation ユーザーガイドのAWS::CodeStarConnections::Connection」を参照してください。

ドキュメント履歴

以下の表は、デベロッパーツールコンソールの今回のリリースの内容をまとめたものです。

- AWS CodeStar Notifications API バージョン: 2019-10-15
- AWS CodeConnections API バージョン: 2023-12-01

変更	説明	日付
接続用の新しい Azure DevOps プロバイダー	Azure DevOps とやり取りするための AWS リソースの接続の設定のサポートが追加されました。詳細については、「Azure DevOps への接続を作成する」を参照してください。	2025 年 8 月 5 日
ホスト VPC IDs の新しい条件キー	VpcId 条件キーを使用して GitHub Enterprise Server および GitLab セルフマネージドホストのホストアクセスを管理できます。条件キーを使用すると、指定された VPC ID を使用するようにホストの作成または更新に関連するポリシーを適用できます。詳細については、「Connections アクセス許可リファレンス」を参照してください。	2025 年 3 月 13 日
アカウント間の接続共有のサポートを追加	で接続をリソースとして表示および管理し AWS Resource Access Manager、接続を共有できます AWS アカウント。詳細については、「 と接続を	2025 年 3 月 6 日

	共有する AWS アカウント」を参照してください。	
更新して、接続がユーザーアカウントまたは組織とどのように連携するかを説明する情報を追加および修正します。	概要とトラブルシューティング情報が更新され、接続がユーザーアカウントまたは組織とどのように連携するかが正しく説明されました。「接続の仕組み」、AWS CodeConnections の接続が組織と連携する方法」、「組織をサポートするインストール済みプロバイダーの接続とホストの設定」を参照してください。	2024 年 12 月 9 日
接続service-linked-roleマネージドポリシーの更新	Git リポジトリとの Git 同期を使用するためのサービスにリンクされたロールの マネージドポリシーが、両方のサービスプレフィックスを持つリソース用に更新されました。詳細については、AWS CodeConnections のサービスにリンクされたロールの使用」および「 マネージドポリシー」を参照してください。	2024 年 4 月 26 日
AWS CodeStar Connections の名前が AWS CodeConnections に変更されました	Introduction AWS CodeConnections を使用すると、CodePipeline のパイプラインなどのリソースと AWS サードパーティーの Git プロバイダー間の接続を作成および管理できます。	2024 年 3 月 29 日

CodeBuild で GitLab への接続がサポートされるようになりました	GitLab への接続を設定するためのサポートが CodeBuild に追加されました。詳細については、AWS CodeConnections との製品とサービスの統合」を参照してください。	2024 年 3 月 27 日
GitLab セルフマネージドのサポート	GitLab セルフマネージドとやり取りする AWS リソースの接続とホストの設定のサポートが追加されました。詳細については、「ホストを作成または更新するワークフロー」と「GitLab セルフマネージドへの接続を作成する」を参照してください。	2023 年 12 月 28 日
接続用の新しいリポジトリリンクと同期設定	リポジトリリンクの設定と同期設定に関する情報を追加しました。同期設定を使用して Git リポジトリのコンテンツを同期し、 CloudFormation スタックリソースを更新します。詳細については、「リポジトリリンクを操作する」と「同期設定を使用する」を参照してください。	2023 年 11 月 27 日
接続のサービスにリンクされたロールのサポート	Git 同期を Git リポジトリで使用するための接続設定のサポートが追加されました。詳細については、AWS CodeConnections のサービスにリンクされたロールの使用」および「 マネージドポリシー」を参照してください。	2023 年 11 月 26 日

GitLab グループのサポート	GitLab グループとやり取りするための AWS リソースの接続の設定のサポートが追加されました。詳細については、Create a connection および Create a connection to GitLab を参照してください。	2023 年 9 月 15 日
新しい GitLab プロバイダータイプ	GitLab への接続を作成できるようになりました。詳細については、Create a connection および Create a connection to GitLab を参照してください。	2023 年 8 月 10 日
通知ルールの新しいターゲットタイプ	通知ルールのターゲットとして、Microsoft Teams チャネル用に設定された AWS Chatbot クライアントを選択できるようになりました。詳細については、「通知ルールの作成」と「通知ルールのターゲットの使用」を参照してください。	2023 年 5 月 17 日
欧州 (ミラノ) リージョンで接続が利用可能に	欧州 (ミラノ) リージョンの接続に関する情報を追加しました。詳細については、「リージョン間の AWS CodeConnections リソース間のトラフィック」を参照してください。	2023 年 5 月 17 日

リポジトリのアクセス許可に関する接続エラーのトラブルシューティングを追加	GitHub 組織のリポジトリへの接続を作成する場合は、GitHub 組織の所有者である必要があります。詳細については、「GitHub への接続時の接続エラー」を参照してください。	2022 年 8 月 29 日
ホストリソースのタグ付けに関する情報を追加	コンソールと CLI を使用して、ホストへのタグ付けができるようになりました。詳細については、AWS CodeConnections でリソースをタグ付けする」を参照してください。	2021 年 4 月 19 日
接続の VPC エンドポイントのサポート	接続で VPC エンドポイントを使用できます。詳細については、AWS CodeConnections」と「インターフェイス VPC エンドポイント (AWS PrivateLink)」を参照してください。	2020 年 11 月 24 日
新しい GitHub および GitHub Enterprise Cloud プロバイダーのタイプ	GitHub および GitHub Enterprise Cloud への接続を作成できるようになりました。詳細については、Create a connection および Create a connection to GitHub を参照してください。	2020 年 9 月 30 日

GitHub Enterprise Server プロバイダータイプとホストリソースを追加	このガイドには、接続のホストリソースに関する情報が追加されました。GitHub Enterprise Server への接続を作成できるようになりました。 接続を作成して作業する方法の詳細については、「Create a connection」および「Working with hosts」を参照してください。これは、デベロッパーツールコンソールのユーザーガイドで説明されている接続機能を備えた一般公開リリースです。	2020 年 6 月 29 日

接続の使用とタグ付けに関する情報を追加	コンソールの接続機能に関する情報が、このガイドに追加されました。概念、開始手順、ポリシーの例を含むアクセス許可に関するリファレンス、接続の作成、表示、およびタグ付けの手順を表示できます。詳細については、「接続とは」、「接続の概念」、「接続の開始方法」、「接続の作成」、AWS CodeConnections のリソースのタグ付け」、「セキュリティ」、「接続のクォータ」、「トラブルシューティング」、およびAWS CodeConnections API コール AWS CloudTrail」を参照してください。追加のプロバイダのアクション（アクセス許可のみのアクション）のリストを表示するには、Actions for ProviderType を参照してください。	2020 年 6 月 28 日
通知ルールの新しいターゲットタイプ	通知ルールのターゲットとして、Slack チャネル用に設定された AWS Chatbot クライアントを選択できるようになりました。詳細については、「通知ルールの作成」と「通知ルールのターゲットの使用」を参照してください。	2020 年 4 月 2 日

追加の AWS CodeCommit イベントに関する通知を追加しました	プルリクエストの承認に関連するイベントの通知を設定できるようになりました。詳細については、「リポジトリでの通知ルールのイベント」および「CodeCommit でのプルリクエストの操作 」を参照してください。	2020 年 2 月 10 日
2 つの追加 AWS リージョンで利用可能な通知	デベロッパーツールコンソールで、中東 (バーレーン) およびアジアパシフィック (香港) の通知をサポートするようになりました。詳細については、「 AWS 全般のリファレンス」の「AWS CodeStar 通知」を参照してください。	2020 年 2 月 5 日
暗号化された Amazon SNS トピックのサポートを追加	暗号化された Amazon SNS トピックを通知ターゲットとして使用するためのガイダンスを追加しました。詳細については、「Configure Amazon SNS topics for notifications」を参照してください。	2020 年 2 月 4 日
通知には、CodeCommit のセッションタグ情報を含めることができる	セッションタグを使用して、CodeCommit の通知に表示名や E メールアドレスなどのユーザー ID 情報を含めることができるようになりました。詳細については、「概念」および「CodeCommit で ID 情報を提供するためのタグの使用」を参照してください。	2019 年 12 月 19 日

初回リリース	これはデベロッパーツールコンソールのユーザーガイドの初回リリースです。	2019 年 11 月 5 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。

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。