デベロッパーガイド

AWS App Runner

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS App Runner: デベロッパーガイド

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon の商標およびトレードドレスはAmazon 以外の製品およびサービスに使用することはできません。また、お客様に誤解を与える可能性がある形式で、または Amazon の信用を損なう形式で使用することもできません。Amazon が所有していないその他のすべての商標は Amazon との提携、関連、支援関係の有無にかかわらず、それら該当する所有者の資産です。

Table of Contents

とは AWS App Runner 1
App Runner とは 1
App Runner へのアクセス 1
App Runner の料金 2
次のステップ 2
設定 3
にサインアップする AWS アカウント 3
管理アクセスを持つユーザーを作成する 4
プログラム的なアクセス権を付与する 5
次のステップ 6
入門 7
前提条件 7
ステップ 1: App Runner サービスを作成する 9
ステップ 2: サービスコードを変更する 19
ステップ 3: 設定を変更する 20
ステップ 4: サービスのログを表示する 22
ステップ 5 : クリーンアップ 25
次のステップ 25
アーキテクチャと概念 27
App Runner の概念 28
App Runner でサポートされている設定 29
App Runner リソース 30
App Runner リソースクォータ 32
イメージベースのサービス 34
イメージリポジトリプロバイダー 34
AWS アカウントの Amazon ECR に保存されているイメージの使用 35
別の AWS アカウントの Amazon ECR に保存されているイメージの使用 35
Amazon ECR Public に保存されているイメージの使用 36
イメージの例 37
コードベースのサービス 38
ソースコードリポジトリプロバイダー 39
ソースコードリポジトリプロバイダーからのデプロイ 39
ソースディレクトリ 40
App Runner マネージドプラットフォーム 41

マネージドランタイムバージョンと App Runner ビルド 41
App Runner のビルドと移行の詳細 42
Python プラットフォーム 46
Python ランタイム設定 48
特定のランタイムバージョンのコールアウト 48
Python ランタイムの例 49
リリース情報 54
Node.js プラットフォーム 55
Node.js ランタイム設定 56
特定のランタイムバージョンのコールアウト 59
Node.js ランタイムの例 59
リリース情報 64
Java プラットフォーム 66
Java ランタイム設定 67
Java ランタイムの例 68
リリース情報 72
.NET プラットフォーム 74
.NET ランタイム設定 75
.NET ランタイムの例 76
リリース情報 78
PHP プラットフォーム 80
PHP ランタイム設定 81
互換性 81
PHP ランタイムの例 83
リリース情報 91
Ruby プラットフォーム 93
Ruby ランタイム設定 94
Ruby ランタイムの例 94
リリース情報 97
Go プラットフォーム 98
Go ランタイム設定 99
Go ランタイムの例 99
リリース情報 101
App Runner の開発 103
ランタイム情報 103
コード開発ガイドライン 105

App Runner コンソール ... 106
コンソール全体のレイアウト ... 106
サービスページ ... 107
サービスダッシュボードページ ... 107
接続されたアカウントページ ... 108
Auto Scaling 設定ページ ... 109
サービスの管理 ... 111
作成 ... 111
前提条件 ... 112
サービスを作成する ... 112
失敗したサービスを再構築する ... 127
App Runner コンソールを使用した失敗した App Runner サービスの再構築 ... 127
App Runner API または を使用した失敗した App Runner サービスの再構築 AWS CLI ... 128
デプロイ ... 129
デプロイ方法 ... 129
手動デプロイ ... 131
設定 ... 133
App Runner API または を使用してサービスを設定する AWS CLI ... 134
App Runner コンソールを使用してサービスを設定する ... 135
App Runner 設定ファイルを使用してサービスを設定する ... 136
オブザーバビリティ設定 ... 136
設定リソース ... 138
ヘルスチェックの設定 ... 140
Connections ... 142
接続の管理 ... 142
Auto scaling ... 144
サービスの自動スケーリングを管理する ... 145
Auto Scaling 設定リソースを管理する ... 147
カスタムドメイン名 ... 154
カスタムドメインをサービスに関連付ける (リンクする) ... 155
カスタムドメインの関連付けを解除 (リンク解除) ... 158
カスタムドメインの管理 ... 159
Amazon Route 53 エイリアスレコードを設定する ... 167
一時停止/再開 ... 169
比較した一時停止と削除 ... 170
サービスが一時停止したとき ... 170

サービスの一時停止と再開 ... 171
削除 ... 173
比較した一時停止と削除 ... 173
App Runner は何を削除しますか？ ... 174
サービスを削除する ... 174
リファレンス環境変数 ... 176
機密データを環境変数として参照する ... 176
考慮事項 ... 177
アクセス許可 ... 178
環境変数を管理する ... 179
App Runner コンソール ... 180
App Runner API または AWS CLI ... 182
ネットワーク ... 188
用語 ... 188
一般的な用語 ... 188
送信トラフィックの設定に固有の用語 ... 189
受信トラフィックの設定に固有の用語 ... 190
受信トラフィック ... 190
ヘッダー ... 191
プライベートエンドポイントを有効にする ... 191
App Runner のパブリックエンドポイントの IPv6 を有効にする ... 205
送信トラフィック ... 210
VPC コネクタ ... 211
サブネット ... 211
セキュリティグループ ... 212
VPC アクセスを管理する ... 213
オブザーバビリティ ... 219
アクティビティ ... 219
App Runner サービスアクティビティを追跡する ... 219
ログ (CloudWatch Logs) ... 221
App Runner ロググループとストリーム ... 221
コンソールでの App Runner ログの表示 ... 223
メトリクス (CloudWatch) ... 225
App Runner メトリクス ... 225
コンソールでの App Runner メトリクスの表示 ... 227
イベント処理 (EventBridge) ... 229

App Runner イベントを処理する EventBridge ルールの作成 230
App Runner イベントの例 230
App Runner イベントパターンの例 232
App Runner イベントリファレンス 233
API アクション (CloudTrail) 235
CloudTrail の App Runner 情報 235
App Runner ログファイルエントリについて 236
トレース (X-Ray) 239
トレース用にアプリケーションを計測する 240
App Runner サービスインスタンスロールに X-Ray アクセス許可を追加する 243
App Runner サービスの X-Ray トレースを有効にする 244
App Runner サービスの X-Ray トレースデータを表示する 244
AWS WAF ウェブ ACL 245
受信ウェブリクエストフロー 245
WAF ウェブ ACLs App Runner サービスに関連付ける 246
考慮事項 247
アクセス許可 248
ウェブ ACLs の管理 249
App Runner コンソール 249
AWS CLI 253
AWS WAF ウェブ ACLsテストとログ記録 258
App Runner 設定ファイル 260
例 261
設定ファイルの例 261
参照資料 264
構造の概要 264
上位セクション 265
ビルドセクション 265
実行セクション 267
App Runner API 272
を使用して App Runner AWS CLI を操作する 272
の使用 AWS CloudShell 272
の IAM アクセス許可の取得 AWS CloudShell 273
を使用した App Runner の操作 AWS CloudShell 274
を使用した App Runner サービスの検証 AWS CloudShell 277
トラブルシューティング 278

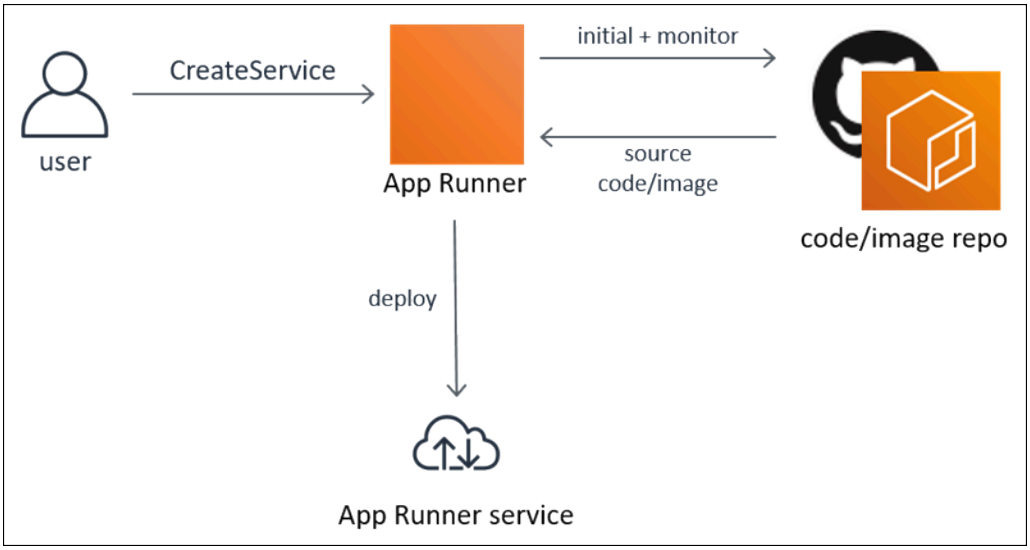
サービスの作成に失敗しました ... 278
カスタムドメイン名 ... 279
カスタムドメインの作成失敗エラーの取得 ... 280
カスタムドメインの DNS 証明書検証保留中エラーの取得 ... 281
基本的なトラブルシューティングコマンド ... 281
カスタムドメイン証明書の更新 ... 282
リクエストルーティングエラー ... 283
404 App Runner サービスエンドポイントに HTTP/HTTPS トラフィックを送信するときにエラーが見つからない ... 283
Amazon RDS またはダウンストリームサービスへの接続が失敗する ... 284
起動またはスケーリングに十分な IP アドレスがない場合 ... 287
サービスを更新して利用可能な IPsを増やす方法 ... 287
サービスに必要な IPsの計算 ... 288
新しいサブネットを作成する (複数可) ... 288
VPC へのセカンダリ CIDR ブロックのアタッチ ... 289
検証 ... 290
一般的な落とし穴 ... 290
その他のリソース ... 291
用語集 ... 291
セキュリティ ... 292
データ保護 ... 293
データの暗号化 ... 294
インターネットのプライバシー ... 295
Identity and Access Management ... 295
対象者 ... 296
アイデンティティを使用した認証 ... 296
ポリシーを使用したアクセスの管理 ... 299
App Runner と IAM ... 302
アイデンティティベースのポリシーの例 ... 311
サービスにリンクされたロールの使用 ... 316
AWS マネージドポリシー ... 324
トラブルシューティング ... 326
ログ記録とモニタリング ... 327
コンプライアンス検証 ... 328
耐障害性 ... 330
インフラストラクチャセキュリティ ... 330

VPC エンドポイント 331
App Runner の VPC エンドポイントの設定 331
VPC ネットワークプライバシーに関する考慮事項 332
エンドポイントポリシーを使用して VPC エンドポイントでアクセスを制御する 332
インターフェイスエンドポイントとの統合 333
責任共有モデル 333
パッチコンテナイメージ 333
セキュリティに関するベストプラクティス 333
予防的セキュリティのベストプラクティス 334
セキュリティ問題の検出ベストプラクティス 334
AWS 用語集 335
..... cccxxxvi

とは AWS App Runner

AWS App Runner は、ソースコードまたはコンテナイメージから AWS クラウドのスケーラブルで安全なウェブアプリケーションに直接デプロイするための、高速でシンプル、かつ費用対効果の高い方法を提供する AWS サービスです。新しいテクノロジーを学習したり、使用するコンピューティングサービスを決定したり、 AWS リソースをプロビジョニングして設定する方法を知っている必要はありません。

App Runner は、コードまたはイメージリポジトリに直接接続します。フルマネージド型のオペレーション、高パフォーマンス、スケーラビリティ、セキュリティを備えた自動統合および配信パイプラインを提供します。



App Runner とは

開発者は、App Runner を使用して、コードまたはイメージリポジトリの新しいバージョンをデプロイするプロセスを簡素化できます。

運用チームの場合、App Runner は、コミットがコードリポジトリにプッシュされるたびに、または新しいコンテナイメージバージョンがイメージリポジトリにプッシュされるたびに、自動デプロイを有効にします。

App Runner へのアクセス

App Runner サービスのデプロイは、次のいずれかのインターフェイスを使用して定義および設定できます。

- App Runner コンソール – App Runner サービスを管理するためのウェブインターフェイスを提供します。
- App Runner API – App Runner アクションを実行するための RESTful API を提供します。詳細については、「AWS App Runner API リファレンス」を参照してください。
- AWS コマンドラインインターフェイス (AWS CLI) – Amazon VPC を含む幅広い AWS のサービス用のコマンドを提供し、Windows、macOS、Linux でサポートされています。詳細については、「AWS Command Line Interface」を参照してください。
- AWS SDKs – 言語固有の APIs を提供し、署名の計算、リクエストの再試行の処理、エラー処理など、接続に関する多くの詳細を処理します。詳細については、AWS SDKを参照してください。

App Runner の料金

App Runner は、アプリケーションを実行するための費用対効果の高い方法を提供します。App Runner サービスが消費するリソースに対してのみ料金が発生します。リクエストトラフィックが少ない場合、サービスはスケールダウンしてコンピューティングインスタンス数を減らします。プロビジョニングされたインスタンスの最小数と最大数、インスタンスが処理する最大負荷など、スケーラビリティ設定を制御できます。

App Runner の自動スケーリングの詳細については、「」を参照してくださいthe section called “Auto scaling”。

料金情報については、「AWS App Runner の料金」を参照してください。

次のステップ

App Runner の使用を開始する方法については、以下のトピックを参照してください。

- 設定 – App Runner を使用するための前提条件となるステップを完了します。
- 入門 – 最初のアプリケーションを App Runner にデプロイします。

App Runner のセットアップ

新規の AWS お客様は、 の使用を開始する前に、このページに記載されているセットアップの前提条件を完了してください AWS App Runner。

これらのセットアップ手順では、 AWS Identity and Access Management (IAM) サービスを使用します。IAM の詳細については、以下の資料を参照してください。

- AWS Identity and Access Management (IAM)
- IAM ユーザーガイド

にサインアップする AWS アカウント

がない場合は AWS アカウント、次の手順を実行して作成します。

にサインアップするには AWS アカウント

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

   サインアップ手順の一環として、通話呼び出し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するように求められます。

   にサインアップすると AWS アカウント、 AWS アカウントのルートユーザー が作成されます。ルートユーザーには、アカウントのすべての AWS のサービス とリソースへのアクセス権があります。セキュリティ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、 のセキュリティを確保し AWS IAM Identity Center、 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 Management Console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 Identity Center ユーザーガイド」の「AWS IAM Identity Center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 Identity Center 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 Identity Center ユーザーガイド」の「権限設定を作成する」を参照してください。

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

   手順については、「AWS IAM Identity Center ユーザーガイド」の「グループの結合」を参照してください。

プログラム的なアクセス権を付与する

ユーザーが の AWS 外部で を操作する場合は、プログラムによるアクセスが必要です AWS Management Console。プログラムによるアクセスを許可する方法は、 がアクセスするユーザーのタイプによって異なります AWS。

ユーザーにプログラマチックアクセス権を付与するには、以下のいずれかのオプションを選択します。

プログラマチックアクセス権を必要とするユーザー	目的	方法
ワークフォースアイデンティティ (IAM アイデンティティセンターで管理されているユーザー)	一時的な認証情報を使用して AWS CLI、、 AWS SDKs、または AWS APIs。	使用するインターフェイスの指示に従ってください。 • については AWS CLI、「 AWS Command Line Interface ユーザーガイド」の「 を使用する AWS CLI ように AWS IAM Identity Centerを設定する」を参照してください。 • AWS SDKs、ツール、API については、 AWS APIs「 SDK およびツールリファ

プログラマチックアクセス権を必要とするユーザー	目的	方法
		レンスガイド」の「IAM アイデンティティセンター認証」を参照してください。 AWS SDKs
IAM	一時的な認証情報を使用して AWS CLI、、 AWS SDKs、または AWS APIs。	「IAM ユーザーガイド」の「 AWS リソースでの一時的な認証情報の使用」の手順に従います。
IAM	(非推奨) 長期認証情報を使用して、AWS CLI、 AWS SDKs、または AWS APIs。	使用するインターフェイスの指示に従ってください。 • については AWS CLI、「 AWS Command Line Interface ユーザーガイド」の「IAM ユーザー認証情報を使用した認証」を参照してください。 • AWS SDKs「 SDK とツールリファレンスガイド」の「長期認証情報を使用した認証」を参照してください。 AWS SDKs • API AWS APIs「IAM ユーザーのアクセスキーの管理」を参照してください。

次のステップ

前提条件のステップを完了しました。最初のアプリケーションを App Runner にデプロイするには、「」を参照してください入門。

App Runner の開始方法

AWS App Runner は、既存のコンテナイメージまたはソースコードを で実行中のウェブ AWS サービスに直接変換するための、高速でシンプル、かつ費用対効果の高い方法を提供する サービスです AWS クラウド。

このチュートリアルでは、 AWS App Runner を使用してアプリケーションを App Runner サービスにデプロイする方法について説明します。ここでは、ソースコードとデプロイ、サービスビルド、サービスランタイムの設定について説明します。また、コードバージョンのデプロイ、設定変更、ログの表示の方法も示します。最後に、チュートリアルの手順に従って作成したリソースをクリーンアップする方法を示します。

トピック

- 前提条件
- ステップ 1: App Runner サービスを作成する
- ステップ 2: サービスコードを変更する
- ステップ 3: 設定を変更する
- ステップ 4: サービスのログを表示する
- ステップ 5 : クリーンアップ
- 次のステップ

前提条件

チュートリアルを開始する前に、必ず次のアクションを実行してください。

1. のセットアップ手順を完了します設定。
2. GitHub リポジトリと Bitbucket リポジトリのどちらを使用するかを決定します。
   - Bitbucket を使用するには、Bitbucket アカウントをまだ作成していない場合は、まず作成します。Bitbucket を初めて使用する場合は、Bitbucket クラウドドキュメントの「Bitbucket の開始方法」を参照してください。
   - GitHub を使用するには、GitHub アカウントをまだ作成していない場合は作成します。GitHub を初めて使用する場合は、GitHub ドキュメントの「GitHub の開始方法GitHub」を参照してください。

> **Note**
>
> アカウントから複数のリポジトリプロバイダーへの接続を作成できます。したがって、GitHub リポジトリと Bitbucket リポジトリの両方からデプロイする手順を繰り返すことができます。次回は、 を使用して新しい App Runner サービスを作成し、他のリポジトリプロバイダー用の新しいアカウント接続を作成します。

3. リポジトリプロバイダーアカウントにリポジトリを作成します。このチュートリアルでは、リポジトリ名 を使用しますpython-hello。次の例で指定された名前とコンテンツを使用して、リポジトリのルートディレクトリにファイルを作成します。

python-hello サンプルリポジトリのファイル

Example requirements.txt

```
pyramid==2.0
```

Example server.py

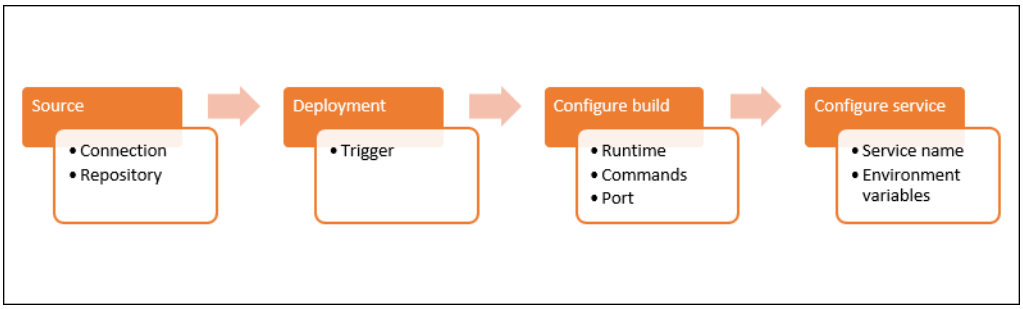
```
from wsgiref.simple_server import make_server
from pyramid.config import Configurator
from pyramid.response import Response
import os

def hello_world(request):
    name = os.environ.get('NAME')
    if name == None or len(name) == 0:
        name = "world"
    message = "Hello, " + name + "!\n"
    return Response(message)

if __name__ == '__main__':
    port = int(os.environ.get("PORT"))
    with Configurator() as config:
        config.add_route('hello', '/')
        config.add_view(hello_world, route_name='hello')
        app = config.make_wsgi_app()
    server = make_server('0.0.0.0', port, app)
    server.serve_forever()
```

ステップ 1: App Runner サービスを作成する

このステップでは、 の一部として GitHub または Bitbucket で作成したサンプルソースコードリポジトリに基づいて App Runner サービスを作成しますthe section called “前提条件”。この例には、シンプルな Python ウェブサイトが含まれています。サービスを作成するために実行する主なステップは次のとおりです。

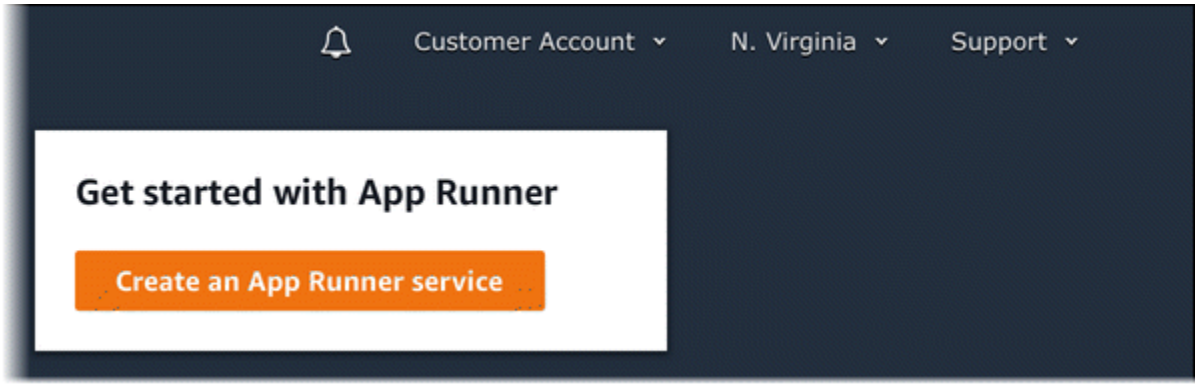
1. ソースコードを設定します。
2. ソースデプロイを設定します。
3. アプリケーションビルドを設定します。
4. サービスを設定します。
5. 確認して確認します。

次の図は、App Runner サービスを作成する手順の概要を示しています。

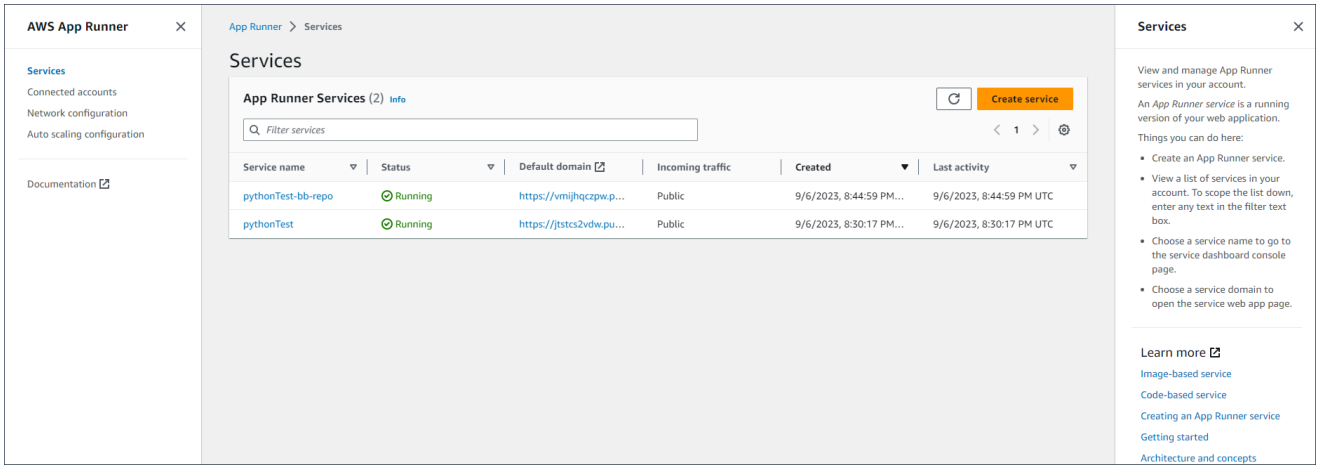


ソースコードリポジトリに基づいて App Runner サービスを作成するには

1. ソースコードを設定します。
   a. App Runner コンソールを開き、リージョンリストで を選択します AWS リージョン。
   b. AWS アカウント に App Runner サービスがまだない場合は、コンソールのホームページが表示されます。App Runner サービスの作成を選択します。



に既存のサービス AWS アカウント がある場合、サービスのリストを含むサービスページが表示されます。[Create service (サービスの作成)] を選択します。



c. 「ソースとデプロイ」ページの「ソース」セクションの「リポジトリタイプ」で、「ソースコードリポジトリ」を選択します。

d. プロバイダータイプを選択します。GitHub または Bitbucket を選択します。

e. 次に、新規追加を選択します。プロンプトが表示されたら、GitHub または Bitbucket の認証情報を入力します。

f. 以前に選択したプロバイダータイプに基づいて、次の一連のステップを選択します。

> **Note**
>
> GitHub の AWS コネクタを GitHub アカウントにインストールする次の手順は、1 回限りのステップです。接続を再利用して、このアカウントのリポジトリに基づいて複数の App Runner サービスを作成できます。既存の接続がある場合は、その接続を選択し、リポジトリの選択にスキップします。
> Bitbucket アカウントの AWS コネクタにも同じことが当てはまります。GitHub と Bitbucket の両方を App Runner サービスのソースコードリポジトリとして使用して

いる場合は、プロバイダーごとに 1 つの AWS Connector をインストールする必要があります。その後、各コネクタを再利用して App Runner サービスをさらに作成できます。

- GitHub の場合は、以下の手順に従います。
  i. 次の画面で、接続名を入力します。
  ii. App Runner で GitHub を初めて使用する場合は、別の をインストールする を選択します。
  iii. AWS Connector for GitHub ダイアログボックスで、プロンプトが表示されたら、GitHub アカウント名を選択します。
  iv. AWS Connector for GitHub を承認するように求められたら、AWS 接続の認可を選択します。
  v. Install AWS Connector for GitHub ダイアログボックスで、インストールを選択します。

     アカウント名は、選択した GitHub アカウント/組織として表示されます。アカウントでリポジトリを選択できるようになりました。
  vi. リポジトリ で、作成したサンプルリポジトリ を選択しますpython-hello。Branch で、リポジトリのデフォルトのブランチ名 (main など) を選択します。
  vii. Source ディレクトリはデフォルト値のままにします。ディレクトリのデフォルトはリポジトリルートです。前の前提条件のステップで、ソースコードをリポジトリのルートディレクトリに保存しました。
- Bitbucket の場合は、以下の手順に従います。
  i. 次の画面で、接続名を入力します。
  ii. App Runner で Bitbucket を初めて使用する場合は、別の をインストールする を選択します。
  iii. アクセスAWS CodeStar リクエストダイアログボックスで、ワークスペースを選択し、Bitbucket 統合 AWS CodeStar のために へのアクセスを許可できます。ワークスペースを選択し、アクセス権の付与を選択します。

iv. 次に、 AWS コンソールにリダイレクトされます。Bitbucket アプリケーションが正しい Bitbucket ワークスペースに設定されていることを確認し、次へを選択します。

v. リポジトリ で、作成したサンプルリポジトリ を選択しますpython-hello。Branch で、リポジトリのデフォルトのブランチ名 (main など) を選択します。

vi. Source ディレクトリはデフォルト値のままにします。ディレクトリのデフォルトはリポジトリルートです。前の前提条件のステップで、ソースコードをリポジトリのルートディレクトリに保存しました。

2. デプロイを設定する: デプロイ設定セクションで、自動を選択し、次へを選択します。

> **Note**
>
> 自動デプロイでは、リポジトリソースディレクトリへの新しいコミットごとに、サービスの新しいバージョンが自動的にデプロイされます。

Source and deployment Info

Choose the source for your App Runner service and the way it's deployed.

Source and deployment

Source

Repository type

- ○ Container registry
  Deploy your service using a container image stored in a container registry.
- ◉ Source code repository
  Deploy your service using the code hosted in a source repository.

Provider
Choose the provider where you host your code repository.

GitHub

Github Connection Info

App Runner deploys your source code by installing an app called "AWS Connector for GitHub" in your account. You can install this app in your main GitHub account or in a GitHub organization.

myGitHub [Add new]

Repository

python-hello

Branch

main

Source directory
The build and start commands will execute in this directory. App Runner defaults to the root directory if you don't specify a directory here.

/

Leading and trailing slashes ("/") are not required. Valid examples: "apps/targetapp", "/apps/targetapp/", "/targetapp"

Deployment settings

Deployment trigger

- ○ Manual
  Start each deployment yourself using the App Runner console or AWS CLI.
- ◉ Automatic
  Every push to this branch that affects files in the specified **Source directory** deploys a new version of your service.

Cancel Next

3. アプリケーションビルドを設定します。

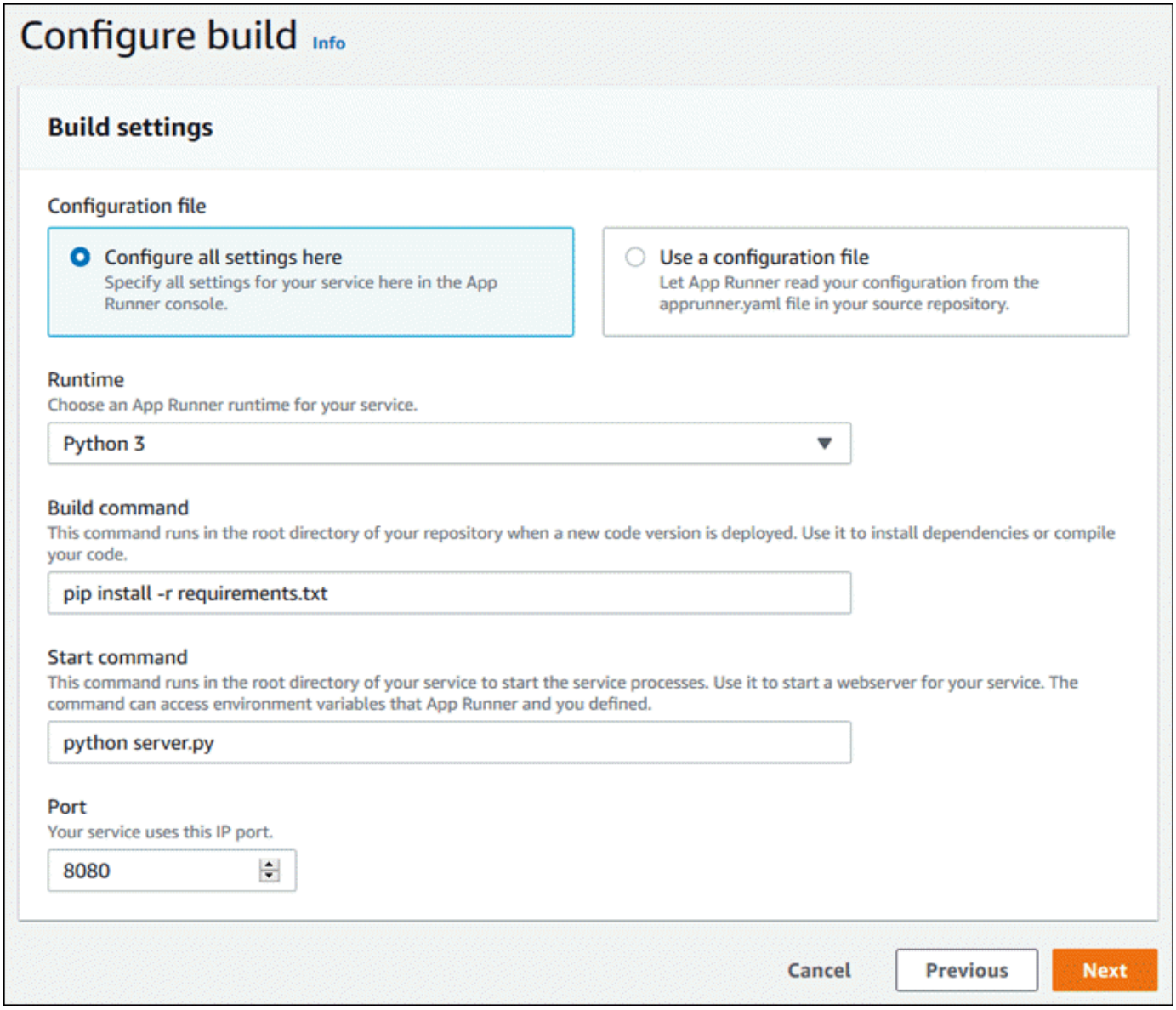
   a. 「ビルドの設定」ページの「設定ファイル」で、「ここですべての設定を構成する」を選択します。

   b. 次のビルド設定を指定します。

      - ランタイム – Python 3 を選択します。
      - ビルドコマンド – と入力します**`pip install -r requirements.txt`**。
      - Start command – と入力します**`python server.py`**。
      - ポート – と入力します**`8080`**。

   c. [Next (次へ)] を選択します。

> **Note**
>
> Python 3 ランタイムは、基本 Python 3 イメージとサンプル Python コードを使用して Docker イメージを構築します。次に、このイメージのコンテナインスタンスを実行するサービスを起動します。



4. サービスを設定します。

   a. 「サービスの設定」ページの「サービス設定」セクションに、サービス名を入力します。

   b. 環境変数 で、環境変数を追加 を選択します。環境変数に次の値を指定します。

      - ソース – プレーンテキストを選択する
      - 環境変数名 – **NAME**
      - 環境変数値 – 任意の名前 (例えば、名) 。

> **Note**
>
> サンプルアプリケーションは、この環境変数で設定した名前を読み取り、ウェブページにその名前を表示します。

c. [Next (次へ)] を選択します。

Configure service Info

Service settings

Service name

python-test

Virtual CPU & memory

1 vCPU | 2 GB

Environment variables — *optional* Info

Add environment variables in plain text or reference them from Secrets Manager and SSM Parameter Store. Update IAM Policies using the IAM Policy template given below to securely reference secrets and configurations as environment variables.

No environment variables have been configured.

Add environment variable

You can add up to 50 more items.

▶ IAM policy templates

▶ Auto scaling Info

Configure automatic scaling behavior.

▶ Health check Info

Configure load balancer health checks.

▶ Security Info

Specify an Instance role and an AWS KMS encryption key

▶ Networking Info

Configure the way your service communicates with other applications, services, and resources.

▶ Observability

Configure observability tooling.

▼ Tags Info

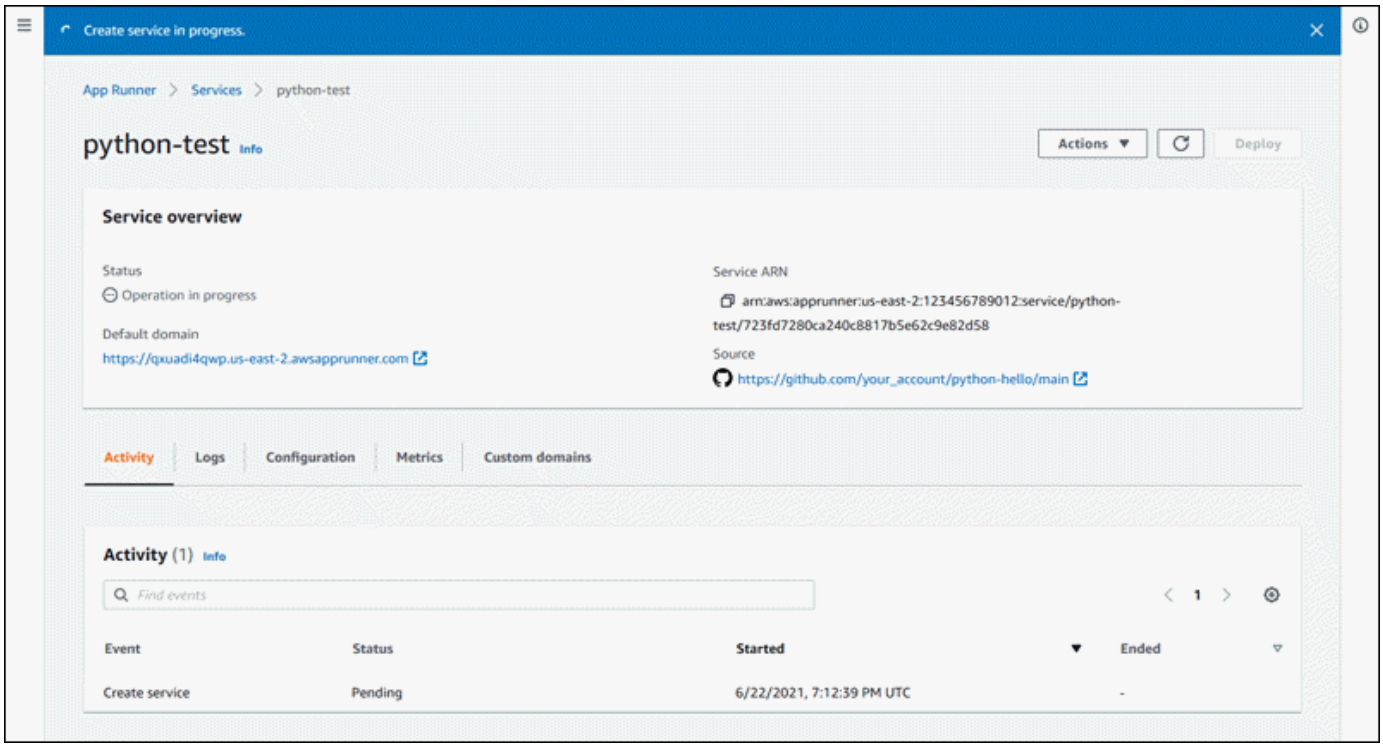
Use tags to search and filter your resources, track your AWS costs, and control access permissions.

Tags — *optional*

A tag is a key-value pair that you assign to an AWS resource.

5. 確認と作成ページで、入力したすべての詳細を確認し、作成とデプロイを選択します。

   サービスが正常に作成されると、コンソールにサービスダッシュボードが表示され、新しいサービスの概要が表示されます。



6. サービスが実行されていることを確認します。

   a. サービスダッシュボードページで、サービスのステータスが実行中になるまで待ちます。

   b. デフォルトのドメイン値を選択します。これはサービスのウェブサイトへの URL です。

> **Note**
>
> App Runner アプリケーションのセキュリティを強化するために、*.awsapprunner.com ドメインはパブリックサフィックスリスト (PSL) に登録されています。セキュリティを強化するために、App Runner アプリケーションのデフォルトドメイン名に機密 Cookie を設定する必要がある場合は、`__Host-`プレフィックス付きの Cookie を使用することをお勧めします。このプラクティスは、クロスサイトリクエストフォージェリ (CSRF) 攻撃からドメインを防ぐ際に役立ちます。詳細については、Mozilla 開発者ネットワークの「Set-Cookie」ページを参照してください。

ウェブページが表示されます: Hello, ***your name***！

ステップ 2: サービスコードを変更する

このステップでは、リポジトリソースディレクトリのコードを変更します。App Runner CI/CD 機能は、変更を自動的に構築してサービスにデプロイします。

サービスコードを変更するには

1. サンプルリポジトリに移動します。
2. という名前のファイルを編集します`server.py`。
3. 変数 に割り当てられた式で`message`、テキストを `Hello` に変更します`Good morning`。
4. 変更を保存してリポジトリにコミットします。
5. 次の手順は、GitHub リポジトリのサービスコードの変更を示しています。
   a. サンプル GitHub リポジトリに移動します。
   b. ファイル名`server.py`を選択して、そのファイルに移動します。
   c. このファイルの編集 (鉛筆アイコン) を選択します。
   d. 変数 に割り当てられた式で`message`、テキストを `Hello` に変更します`Good morning`。

e. [Commit changes] (変更のコミット) を選択します。

6. 新しいコミットが App Runner サービスのデプロイを開始します。サービスダッシュボードページで、サービスのステータスが進行中のオペレーションに変わります。

   デプロイが終了するのを待ちます。サービスダッシュボードページで、サービスのステータスが実行中に戻ります。

7. デプロイが成功したことを確認する: サービスのウェブページが表示されるブラウザタブを更新します。

   このページに、変更後のメッセージ「おはよう、***##***」が表示されるようになりました。

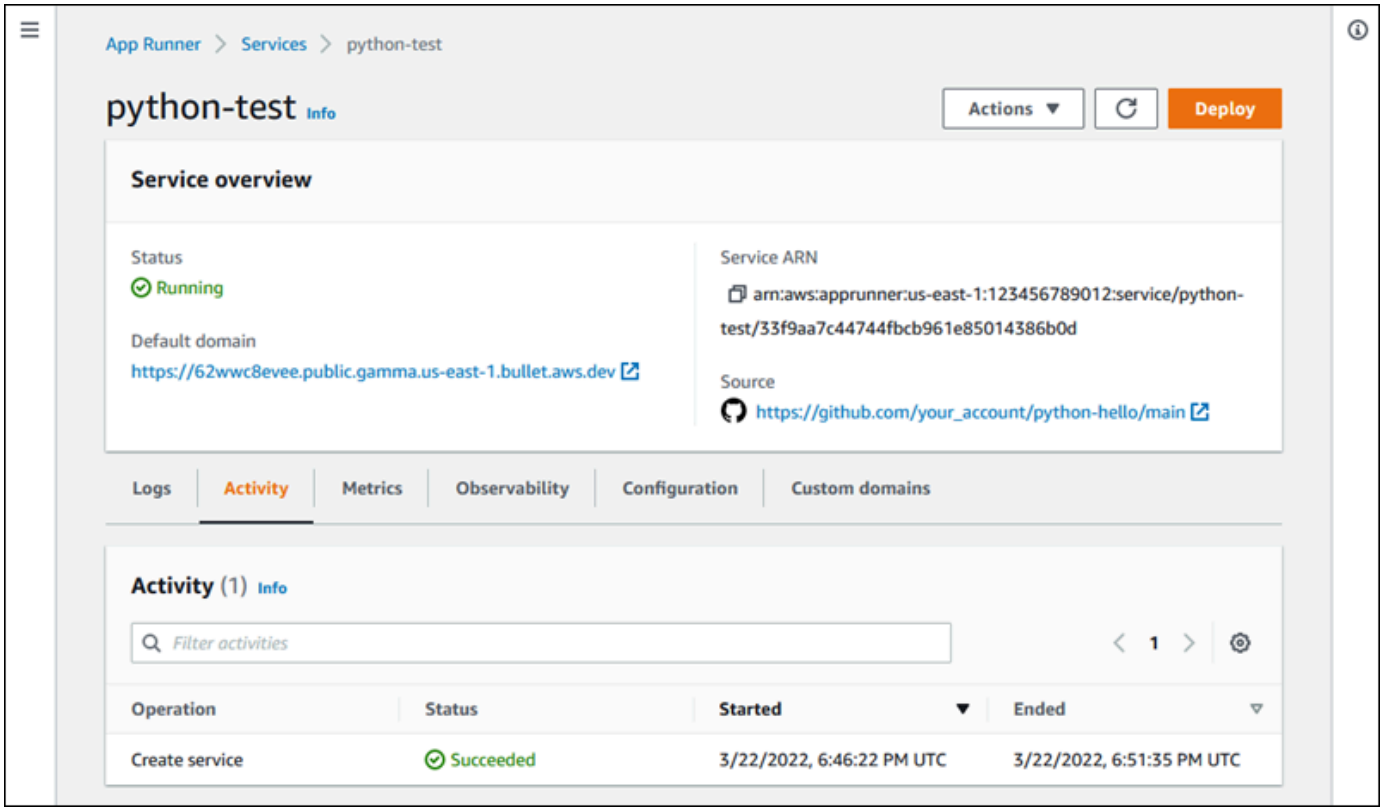
ステップ 3: 設定を変更する

このステップでは、 **NAME**環境変数の値を変更して、サービス設定の変更を示します。

環境変数の値を変更するには

1. App Runner コンソールを開き、リージョンリストで を選択します AWS リージョン。
2. ナビゲーションペインで、サービスを選択し、App Runner サービスを選択します。

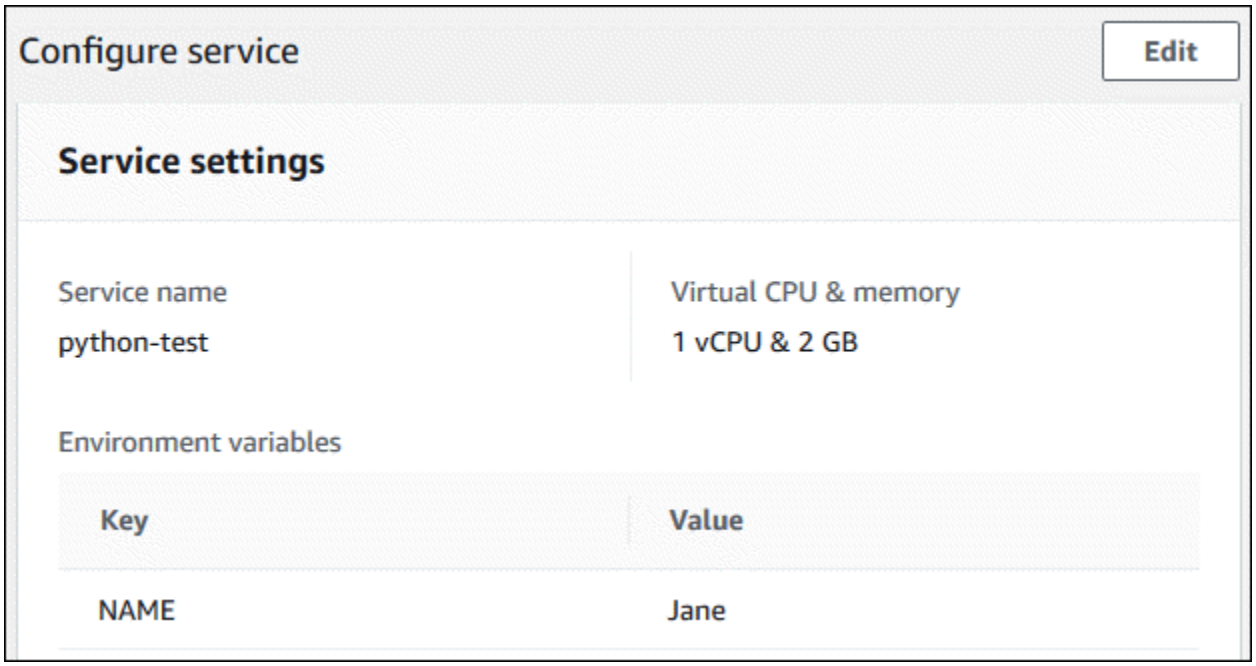
   コンソールには、サービスダッシュボードにサービスの概要が表示されます。



3. サービスダッシュボードページで、設定タブを選択します。

   コンソールには、サービス設定がいくつかのセクションに表示されます。

4. サービスの設定セクションで、編集を選択します。



5. キーが の環境変数の場合**NAME**、値を別の名前に変更します。

6. [Apply changes (変更の適用)] を選択します。

   App Runner は更新プロセスを開始します。サービスダッシュボードページで、サービスのステータスが進行中のオペレーションに変わります。

7. 更新が終了するのを待ちます。サービスダッシュボードページで、サービスのステータスが実行中に戻ります。

8. 更新が成功したことを確認する: サービスのウェブページが表示されるブラウザタブを更新します。

   このページに、変更後の名前「おはよう、*#####*」が表示されるようになりました。

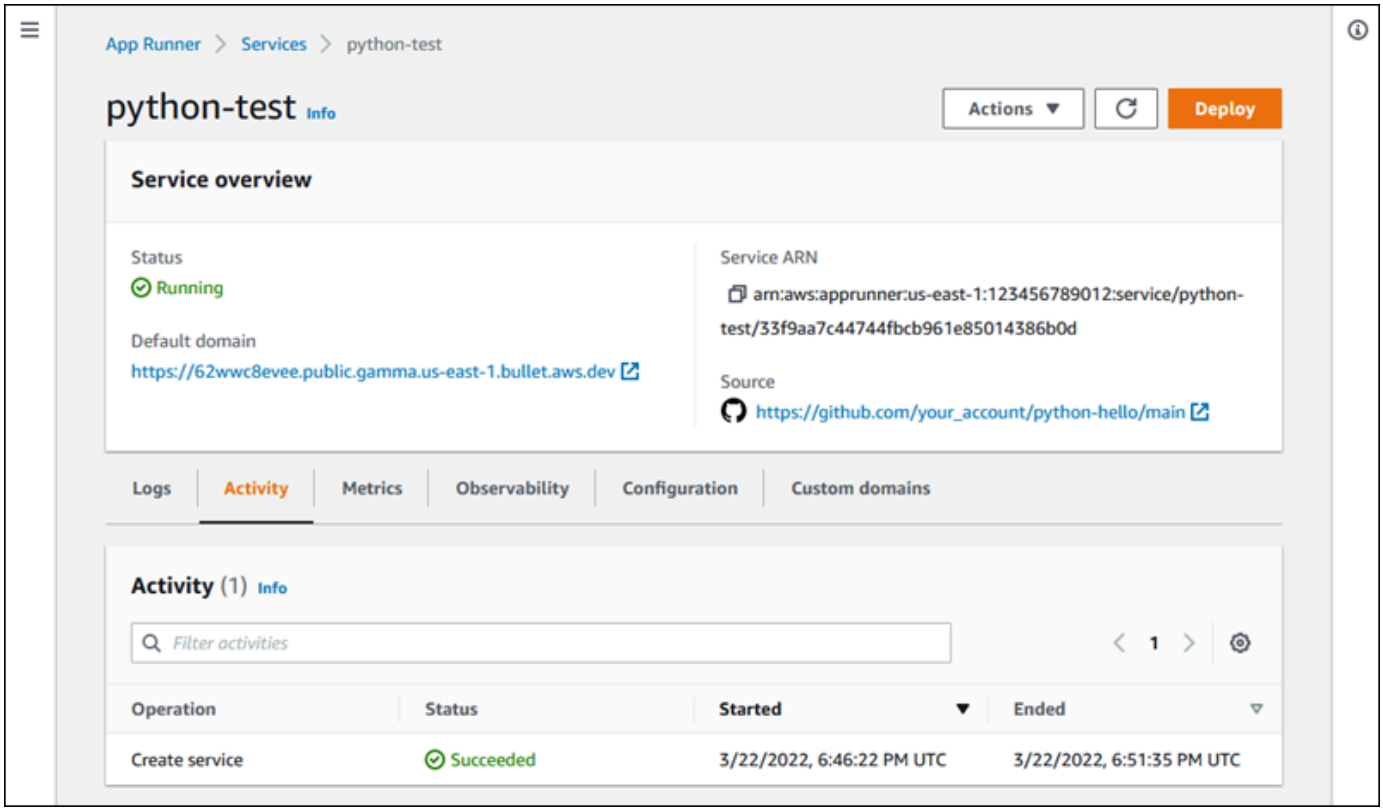
ステップ 4: サービスのログを表示する

このステップでは、App Runner コンソールを使用して App Runner サービスのログを表示します。App Runner は、ログを Amazon CloudWatch Logs (CloudWatch Logs) にストリーミングし、サービスのダッシュボードに表示します。App Runner ログの詳細については、「」を参照してくださいthe section called “ログ (CloudWatch Logs)”。

サービスのログを表示するには

1. App Runner コンソールを開き、リージョンリストで を選択します AWS リージョン。
2. ナビゲーションペインで、サービスを選択し、App Runner サービスを選択します。

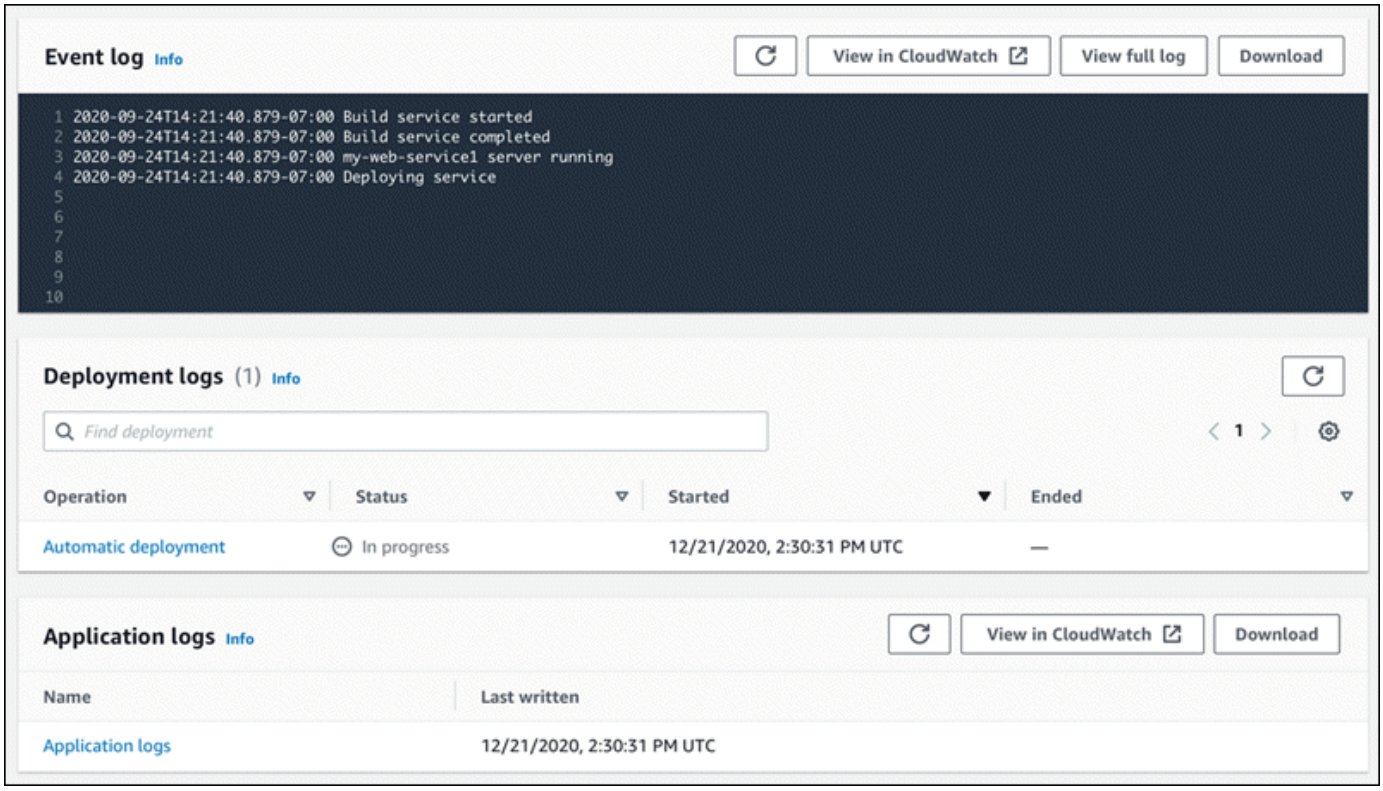
   コンソールには、サービスダッシュボードにサービスの概要が表示されます。



3. サービスダッシュボードページで、ログタブを選択します。

   コンソールには、いくつかのセクションにいくつかのタイプのログが表示されます。

   - イベントログ – App Runner サービスのライフサイクル内のアクティビティ。コンソールに最新のイベントが表示されます。
   - デプロイログ – App Runner サービスへのソースリポジトリのデプロイ。コンソールには、デプロイごとに個別のログストリームが表示されます。
   - アプリケーションログ – App Runner サービスにデプロイされたウェブアプリケーションの出力。コンソールは、実行中のすべてのインスタンスからの出力を 1 つのログストリームに結合します。



4. 特定のデプロイを検索するには、検索語を入力してデプロイログリストの範囲を絞り込みます。テーブルに表示される任意の値を検索できます。
5. ログのコンテンツを表示するには、フルログの表示 (イベントログ) またはログストリーム名 (デプロイログとアプリケーションログ) を選択します。
6. ダウンロードを選択してログをダウンロードします。デプロイログストリームの場合は、まずログストリームを選択します。
7. CloudWatch で表示 を選択して CloudWatch コンソールを開き、その完全な機能を使用して App Runner サービスログを調べます。デプロイログストリームの場合は、まずログストリームを選択します。

> **Note**
>
> CloudWatch コンソールは、結合されたアプリケーションログではなく、特定のインスタンスのアプリケーションログを表示する場合に特に便利です。

ステップ 5：クリーンアップ

これで、App Runner サービスの作成、ログの表示、およびいくつかの変更を行う方法を学習しました。このステップでは、サービスを削除して、不要になったリソースを削除します。

サービスを削除するには

1. サービスダッシュボードページで、アクションを選択し、サービスの削除を選択します。
2. 確認ダイアログで、リクエストされたテキストを入力し、削除を選択します。

   結果: コンソールはサービスページに移動します。削除したサービスのステータスが DELETING と表示されます。しばらくすると、リストから消えます。

このチュートリアルの一部として作成した GitHub および Bitbucket 接続も削除することを検討してください。詳細については、「the section called “Connections”」を参照してください。

次のステップ

最初の App Runner サービスをデプロイしたので、以下のトピックで詳細を確認してください。

- アーキテクチャと概念 – App Runner に関連するアーキテクチャ、主要な概念、 AWS リソース。
- イメージベースのサービス および コードベースのサービス – App Runner がデプロイできる 2 種類のアプリケーションソース。
- App Runner の開発 – App Runner にデプロイするためのアプリケーションコードを開発または移行する際に知っておくべきこと。
- App Runner コンソール – App Runner コンソールを使用してサービスを管理およびモニタリングします。
- サービスの管理 – App Runner サービスのライフサイクルを管理します。
- オブザーバビリティ – メトリクスのモニタリング、ログの読み取り、イベントの処理、サービスアクションコールの追跡、HTTP コールなどのアプリケーションイベントの追跡により、App Runner サービスオペレーションを可視化します。
- App Runner 設定ファイル – App Runner サービスのビルドおよびランタイム動作のオプションを指定する設定ベースの方法です。
- App Runner API – App Runner アプリケーションプログラミングインターフェイス (API) を使用して、App Runner リソースを作成、読み取り、更新、削除します。

- セキュリティ – App Runner やその他の サービスの使用中に AWS と がクラウドセキュリティを確保するさまざまな方法。

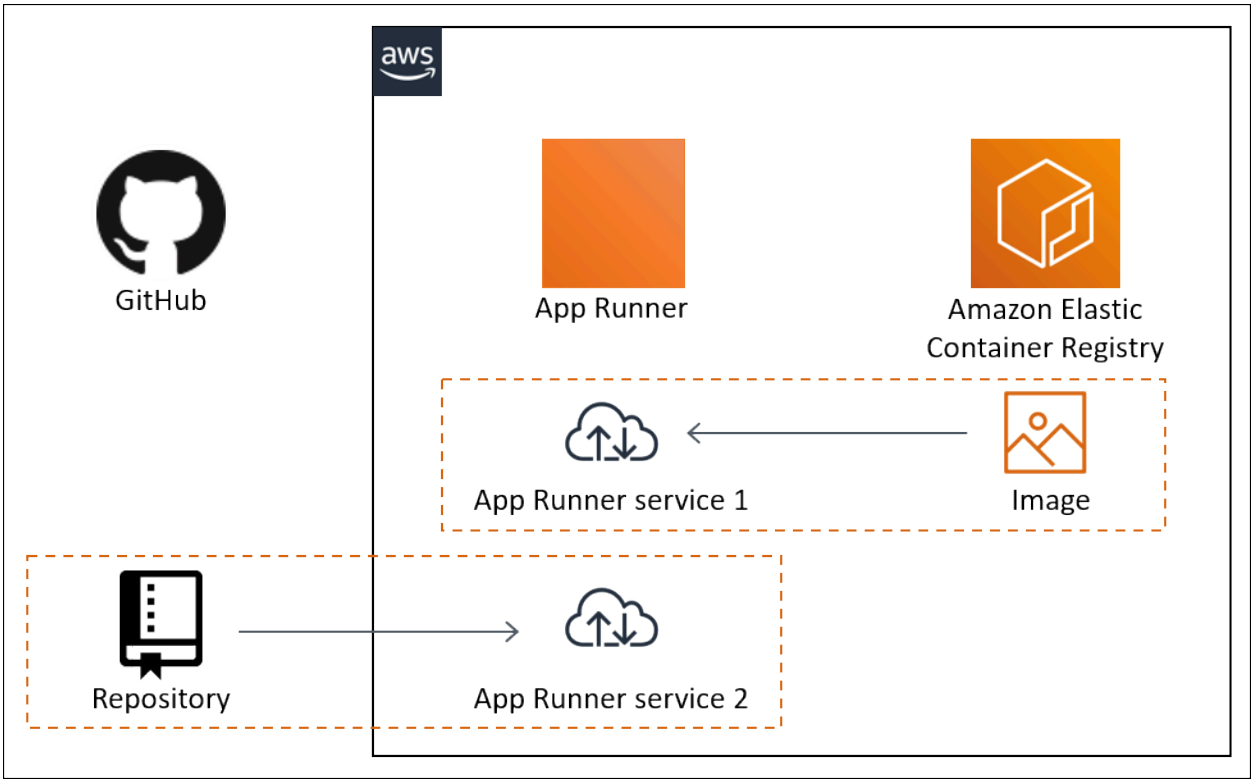
App Runner のアーキテクチャと概念

AWS App Runner は、リポジトリからソースコードまたはソースイメージを取得し、 で実行中のウェブサービスを作成して維持します AWS クラウド。通常、サービスを作成するには、App Runner アクション CreateService を 1 つだけ呼び出す必要があります。

ソースイメージリポジトリでは、App Runner がウェブサービスを実行するためにデプロイできる ready-to-useコンテナイメージを提供します。ソースコードリポジトリでは、ウェブサービスを構築して実行するためのコードと手順を提供し、特定のランタイム環境をターゲットにします。App Runner は、複数のプログラミングプラットフォームをサポートしています。各プラットフォームには、プラットフォームのメジャーバージョン用の 1 つ以上のマネージドランタイムがあります。

現時点では、App Runner は Bitbucket または GitHub リポジトリからソースコードを取得することも、 の Amazon Elastic Container Registry (Amazon ECR) からソースイメージを取得することもできます AWS アカウント。

次の図は、App Runner サービスアーキテクチャの概要を示しています。この図には、2 つのサンプルサービスがあります。1 つは GitHub からソースコードをデプロイし、もう 1 つは Amazon ECR からソースイメージをデプロイします。Bitbucket リポジトリにも同じフローが適用されます。



App Runner の概念

App Runner で実行されているウェブサービスに関連する主要な概念を次に示します。

- App Runner サービス – App Runner がソースコードリポジトリまたはコンテナイメージに基づいてアプリケーションをデプロイおよび管理するために使用する AWS リソース。App Runner サービスは、実行中のアプリケーションのバージョンです。サービスの作成の詳細については、「」を参照してくださいthe section called “作成”。
- ソースタイプ – App Runner サービスをデプロイするために指定するソースリポジトリのタイプ: ソースコードまたはソースイメージ。
- リポジトリプロバイダー – アプリケーションソースを含むリポジトリサービス (GitHub、Bitbucket、Amazon ECR など) 。
- App Runner 接続 – App Runner がリポジトリプロバイダーアカウント (GitHub アカウントや組織など) にアクセスできるようにする AWS リソース。接続の詳細については、「the section called “Connections”」を参照してください。
- ランタイム – ソースコードリポジトリをデプロイするためのベースイメージ。App Runner は、さまざまなプログラミングプラットフォームとバージョンに対してさまざまなマネージドランタイムを提供します。詳細については、「コードベースのサービス」を参照してください。
- デプロイ — ソースリポジトリ (コードまたはイメージ) のバージョンを App Runner サービスに適用するアクション。サービスへの最初のデプロイは、サービスの作成の一環として行われます。それ以降のデプロイは、次の 2 つの方法のいずれかで行うことができます。
  - 自動デプロイ — CI/CD 機能。App Runner サービスを設定して、アプリケーションの各バージョンをリポジトリに表示されるとおりに自動的に構築 (ソースコード用) してデプロイできます。これは、ソースコードリポジトリの新しいコミットでも、ソースイメージリポジトリの新しいイメージバージョンでもかまいません。
  - 手動デプロイ — 明示的に開始する App Runner サービスへのデプロイ。
- カスタムドメイン – App Runner サービスに関連付けるドメイン。ウェブアプリケーションのユーザーは、このドメインを使用して、デフォルトの App Runner サブドメインの代わりにウェブサービスにアクセスできます。詳細については、「the section called “カスタムドメイン名”」を参照してください。

> **Note**
>
> App Runner アプリケーションのセキュリティを強化するために、*.awsapprunner.com ドメインはパブリックサフィックスリスト (PSL) に登録されています。セキュリティを強化するために、App Runner アプリケーションのデフォルトドメイン名に機密 Cookie を設

定する必要がある場合は、__Host-プレフィックス付きの Cookie を使用することをお勧めします。このプラクティスは、クロスサイトリクエストフォージェリ (CSRF) 攻撃からドメインを防ぐ際に役立ちます。詳細については、Mozilla 開発者ネットワークの「Set-Cookie」ページを参照してください。

- メンテナンス – App Runner が App Runner サービスを実行するインフラストラクチャで時折実行するアクティビティ。メンテナンスが進行中の場合、サービスステータスは一時的に OPERATION_IN_PROGRESS (コンソールで進行中のオペレーション) に数分変わります。サービスに対するアクション (デプロイ、設定の更新、一時停止/再開、削除など) は、この間ブロックされます。サービスステータスが に戻ったら、数分後にもう一度 アクションを試してください RUNNING。

> **Note**
> アクションが失敗しても、App Runner サービスがダウンしているわけではありません。アプリケーションはアクティブで、リクエストの処理を継続します。サービスでダウンタイムが発生する可能性はほとんどありません。

特に、App Runner は、サービスをホストしている基盤となるハードウェアの問題を検出すると、サービスを移行します。サービスのダウンタイムを防ぐため、App Runner は新しいインスタンスセットにサービスをデプロイし、トラフィックをそのインスタンスにシフトします (ブルー/グリーンデプロイ) 。料金が一時的にわずかに増加することがあります。

App Runner でサポートされている設定

App Runner サービスを設定するときは、サービスに割り当てる仮想 CPU とメモリの設定を指定します。選択したコンピューティング設定に基づいて支払います。料金の詳細については、AWS Resource Groups 料金表を参照してください。

次の表は、App Runner がサポートする vCPU とメモリの設定に関する情報を示しています。

CPU	「メモリ」
0.25 vCPU	0.5 GB
0.25 vCPU	1 GB

CPU	「メモリ」
0.5 vCPU	1 GB
1 vCPU	2 GB
1 vCPU	3 GB
1 vCPU	4 GB
2 vCPU	4 GB
2 vCPU	6 GB
4 vCPU	8 GB
4 vCPU	10 GB
4 vCPU	12 GB

App Runner リソース

App Runner を使用する場合は、 でいくつかのタイプのリソースを作成および管理します AWS アカウント。これらのリソースは、コードにアクセスし、サービスを管理するために使用されます。

次の表に、これらのリソースの概要を示します。

リソース名	説明
Service	実行中のバージョンのアプリケーションを表します。このガイドの残りの部分では、サービスタイプ、管理、設定、モニタリングについて説明します。 ARN: `arn:aws:apprunner:` *`region`*`:`*`account-id`* `:service/` *`service-name`* `[/`*`service-id`*` ]`
Connection	App Runner サービスに、サードパーティープロバイダーに保存されているプライベートリポジトリへのアクセスを提供します。複数のサービス間で共有するための個別のリソースとして存在します。接続の詳

リソース名	説明
	細については、「the section called “Connections”」を参照してください。 ARN: `arn:aws:apprunner:` *`region`*`:`*`account-id`*` :connection/` *`connection-name`* `[/`*`connection-id`*` ]`
AutoScalingConfiguration	App Runner サービスに、アプリケーションの自動スケーリングを制御する設定を提供します。複数のサービス間で共有するための個別のリソースとして存在します。 Auto Scaling の詳細については、「」を参照してくださいthe section called “Auto scaling”。 ARN: `arn:aws:apprunner:` *`region`*`:`*`account-id`*` :autoscalingconfiguration/` *`config-name`* `[/`*`config-revision`* `[/`*`config-id`*` ]]`
ObservabilityConfiguration	App Runner サービスの追加のアプリケーションオブザーバビリティ機能を設定します。複数のサービス間で共有するための個別のリソースとして存在します。オブザーバビリティ設定の詳細については、「」を参照してくださいthe section called “オブザーバビリティ設定”。 ARN: `arn:aws:apprunner:` *`region`*`:`*`account-id`*` :observabilityconfiguration/` *`config-name`* `[/`*`config-revision`* `[/`*`config-id`*` ]]`
VpcConnector	App Runner サービスの VPC 設定を構成します。複数のサービス間で共有するための個別のリソースとして存在します。VPC 機能の詳細については、「」を参照してくださいthe section called “送信トラフィック”。 ARN: `arn:aws:apprunner:` *`region`*`:`*`account-id`*` :vpcconnector/` *`connector-name`* `[/`*`connector-revision`* `[/`*`connector-id`*` ]]`

リソース名	説明
VpcIngressConnection	これは、受信トラフィックを設定するために使用される AWS App Runner リソースです。VPC インターフェイスエンドポイントと App Runner サービス間の接続を確立し、Amazon VPC 内からのみ App Runner サービスにアクセスできるようにします。VPCIngressConnection の機能の詳細については、「」を参照してくださいthe section called “プライベートエンドポイントを有効にする”。 ARN: `arn:aws:apprunner:` *`region`*`:`*`account-id`*` :vpcingressconnection/` *`vpc-ingress-connection-name`* ` [/`*`connector-id`*` ]]`

App Runner リソースクォータ

AWS は、各 の AWS リソース使用量について、アカウントにいくつかのクォータ (制限とも呼ばれます) を課します AWS リージョン。次の表に、App Runner リソースに関連するクォータを示します。クォータは、 AWS App Runner のエンドポイントとクォータにも記載されていますAWS 全般のリファレンス。

リソースクォータ		説明	デフォルト値	調整可能ですか？
Services		アカウントで作成できるサービスの最大数 AWS リージョン。	30	✓ はい
Connections		各アカウントで作成できる接続の最大数 AWS リージョン。単一の接続を複数のサービスで使用できます。	10	✓ はい
Auto scaling configurations	名前	各アカウントで作成する Auto Scaling 設定で指定できる一意の名前の最大数 AWS リージョン。単一の Auto Scaling 設定を複数のサービスで使用きます。	10	✓ はい
	名前あたりの	一意の名前 AWS リージョン ごとにアカウントで作成できる Auto Scaling 設定リビジョンの最	5	×いいえ

リソースクォータ		説明	デフォルト値	調整可能ですか？
	リビジョン	大数。1 つの Auto Scaling 設定リビジョンを複数のサービスで使用できます。		
Observability configurations	名前	アカウントで各 用に作成するオブザーバビリティ設定で持つことができる一意の名前の最大数 AWS リージョン。単一の可観測性設定を複数のサービスで使用できます。	10	✓ はい
	名前あたりのリビジョン	AWS リージョン 一意の名前ごとにアカウントで作成できるオブザーバビリティ設定リビジョンの最大数。1 つのオブザーバビリティ設定リビジョンを複数のサービスで使用できます。	10	× いいえ
VPC connectors		アカウントで作成できる VPC コネクタの最大数 AWS リージョン。単一の VPC コネクタを複数のサービスで使用できます。	10	✓ はい
VPC Ingress Connection		アカウントで作成できる VPC イングレス接続の最大数 AWS リージョン。単一の VPC Ingress Connection を使用して、複数の App Runner サービスにアクセスできます。	1	× いいえ

ほとんどのクォータは調整可能で、クォータの引き上げをリクエストできます。詳細については、Service Quotas ユーザーガイドの「Requesting a quota increase (クォータの引き上げのリクエスト)」を参照してください。

ソースイメージに基づく App Runner サービス

を使用して AWS App Runner 、ソースコードとソースイメージの 2 つの根本的に異なるタイプのサービスソースに基づいてサービスを作成および管理できます。ソースタイプにかかわらず、App Runner はサービスの起動、実行、スケーリング、ロードバランシングを処理します。App Runner の CI/CD 機能を使用して、ソースイメージまたはコードの変更を追跡できます。App Runner は、変更を検出すると、自動的に (ソースコード用) をビルドし、新しいバージョンを App Runner サービスにデプロイします。

この章では、ソースイメージに基づく のサービスについて説明します。ソースコードに基づくサービスの詳細については、「」を参照してくださいコードベースのサービス。

ソースイメージは、イメージリポジトリに保存されているパブリックまたはプライベートコンテナイメージです。App Runner をイメージにポイントすると、このイメージに基づいてコンテナを実行するサービスが開始されます。ビルドステージは必要ありません。むしろ、ready-to-deployイメージを提供します。

> **Note**
>
> コンテナイメージを提供する場合、これらのイメージを定期的に更新してパッチを適用する責任があります。App Runner がインフラストラクチャを管理する間は、提供されたコンテナイメージのセキュリティとup-to-dateステータスを確認する必要があります。詳細については、AWS App Runner ドキュメントを参照してください。

イメージリポジトリプロバイダー

App Runner は以下のイメージリポジトリプロバイダーをサポートしています。

- Amazon Elastic Container Registry (Amazon ECR) – プライベートなイメージを に保存します AWS アカウント。
- Amazon Elastic Container Registry Public (Amazon ECR Public) – パブリックに読み取り可能なイメージを保存します。

プロバイダーのユースケース

- AWS アカウントの Amazon ECR に保存されているイメージの使用

- 別の AWS アカウントの Amazon ECR に保存されているイメージの使用
- Amazon ECR Public に保存されているイメージの使用

AWS アカウントの Amazon ECR に保存されているイメージの使用

Amazon ECR はイメージをリポジトリに保存します。プライベートリポジトリとパブリックリポジトリがあります。プライベートリポジトリから App Runner サービスにイメージをデプロイするには、App Runner に Amazon ECR からイメージを読み取るアクセス許可が必要です。App Runner にそのアクセス許可を付与するには、App Runner にアクセスロールを提供する必要があります。これは、必要な Amazon ECR アクションのアクセス許可を持つ AWS Identity and Access Management (IAM) ロールです。App Runner コンソールを使用してサービスを作成する場合、アカウント内の既存のロールを選択できます。または、IAM コンソールを使用して新しいカスタムロールを作成することもできます。または、App Runner コンソールで 管理ポリシーに基づいてロールを作成することもできます。

App Runner API または を使用する場合は AWS CLI、2 ステップのプロセスを完了します。まず、IAM コンソールを使用してアクセスロールを作成します。App Runner が提供する管理ポリシーを使用するか、独自のカスタムアクセス許可を入力できます。次に、CreateService API アクションを使用して、サービスの作成時にアクセスロールを指定します。

App Runner サービスの作成については、「」を参照してくださいthe section called “作成”。

別の AWS アカウントの Amazon ECR に保存されているイメージの使用

App Runner サービスを作成するときは、サービスが存在するアカウント以外の AWS アカウントに属する Amazon ECR リポジトリに保存されているイメージを使用できます。クロスアカウントイメージを使用する場合は、前のセクションでリストした同じアカウントイメージに関する考慮事項に加えて、いくつかの考慮事項があります。

- クロスアカウントリポジトリには、ポリシーがアタッチされている必要があります。リポジトリポリシーは、リポジトリ内のイメージを読み取るアクセス許可をアクセスロールに付与します。この目的には、次のポリシーを使用します。をアクセスロールの Amazon リソースネーム (ARN) *access-role-arn*に置き換えます。

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

```
      "Effect": "Allow",
      "Principal": {
        "AWS": "access-role-arn"
      },
      "Action": [
        "ecr:BatchGetImage",
        "ecr:DescribeImages",
        "ecr:GetDownloadUrlForLayer"
      ]
    }
  ]
}
```

リポジトリポリシーを Amazon ECR リポジトリにアタッチする方法については、「Amazon Elastic Container Registry ユーザーガイド」の「リポジトリポリシーステートメントの設定」を参照してください。

- App Runner は、サービスがあるアカウントとは異なるアカウントの Amazon ECR イメージの自動デプロイをサポートしていません。

Amazon ECR Public に保存されているイメージの使用

Amazon ECR Public は、パブリックに読み取り可能なイメージを保存します。以下は、App Runner サービスのコンテキストで注意すべき Amazon ECR と Amazon ECR Public の主な違いです。

- Amazon ECR Public イメージはパブリックに読み取り可能です。Amazon ECR Public イメージに基づいてサービスを作成するときに、アクセスロールを提供する必要はありません。リポジトリにアタッチされたポリシーは必要ありません。
- App Runner は、Amazon ECR Public イメージの自動 (継続的な) デプロイをサポートしていません。

Amazon ECR Public から直接サービスを起動する

App Runner で実行されているウェブサービスとして、Amazon ECR Public Gallery でホストされている互換性のあるウェブアプリケーションのコンテナイメージを直接起動できます。ギャラリーを参照するときは、ギャラリーページで Launch with App Runner を探してイメージを探します。このオプションを含むイメージは App Runner と互換性があります。ギャラリーの詳細については、「Amazon ECR Public ユーザーガイド」の「Amazon ECR Public Gallery の使用」を参照してください。

App Runner サービスとしてギャラリーイメージを起動するには

1. イメージのギャラリーページで、App Runner で起動を選択します。

   結果: App Runner コンソールが新しいブラウザタブで開きます。コンソールにはサービスの作成ウィザードが表示され、必要な新しいサービスの詳細のほとんどが事前に入力されています。
2. コンソールに表示されるリージョン以外の AWS リージョンでサービスを作成する場合は、コンソールヘッダーに表示されるリージョンを選択します。次に、別のリージョンを選択します。
3. ポートには、イメージアプリケーションがリッスンするポート番号を入力します。通常、イメージのギャラリーページにあります。
4. 必要に応じて、その他の設定の詳細を変更します。
5. 次へ を選択し、設定を確認し、作成とデプロイ を選択します。

イメージの例

App Runner チームは、hello-app-runner サンプルイメージを Amazon ECR Public Gallery に保持しています。この例を使用して、イメージベースの App Runner サービスの作成を開始できます。詳細については、「hello-app-runner」を参照してください。

ソースコードに基づく App Runner サービス

を使用して AWS App Runner 、ソースコードとソースイメージの 2 つの根本的に異なるタイプのサービスソースに基づいてサービスを作成および管理できます。ソースタイプに関係なく、App Runner はサービスの起動、実行、スケーリング、ロードバランシングを行います。App Runner の CI/CD 機能を使用して、ソースイメージまたはコードの変更を追跡できます。App Runner は変更を検出すると、自動的に (ソースコード用) ビルドし、新しいバージョンを App Runner サービスにデプロイします。

この章では、ソースコードに基づくサービスについて説明します。ソースイメージに基づくサービスの詳細については、「」を参照してくださいイメージベースのサービス。

ソースコードは、App Runner が構築してデプロイするアプリケーションコードです。App Runner をコードリポジトリ内のソースディレクトリにポイントし、プログラミングプラットフォームのバージョンに対応する適切なランタイムを選択します。App Runner は、ランタイムのベースイメージとアプリケーションコードに基づいてイメージを構築します。次に、このイメージに基づいてコンテナを実行するサービスを開始します。

App Runner は、プラットフォーム固有の便利なマネージドランタイムを提供します。これらの各ランタイムは、ソースコードからコンテナイメージを構築し、言語ランタイムの依存関係をイメージに追加します。Dockerfile などのコンテナ設定やビルド手順を指定する必要はありません。

この章のサブトピックでは、App Runner がサポートするさまざまなプラットフォームについて説明します。これは、さまざまなプログラミング環境とバージョンにマネージドランタイムを提供するマネージドプラットフォームです。

トピック

- ソースコードリポジトリプロバイダー
- ソースディレクトリ
- App Runner マネージドプラットフォーム
- マネージドランタイムバージョンと App Runner ビルド
- Python プラットフォームを使用する
- Node.js プラットフォームを使用する
- Java プラットフォームの使用
- .NET プラットフォームを使用する

- PHP プラットフォームを使用する
- Ruby プラットフォームを使用する
- Go プラットフォームを使用する

ソースコードリポジトリプロバイダー

App Runner は、ソースコードリポジトリから読み取ってソースコードをデプロイします。App Runner はGitHub と Bitbucket の 2 つのソースコードリポジトリプロバイダーをサポートしています。

ソースコードリポジトリプロバイダーからのデプロイ

ソースコードリポジトリから App Runner サービスにソースコードをデプロイするために、App Runner はそれへの接続を確立します。App Runner コンソールを使用してサービスを作成するときは、App Runner がソースコードをデプロイするための接続の詳細とソースディレクトリを指定します。

Connections

サービス作成手順の一部として接続の詳細を指定します。App Runner API または を使用する場合 AWS CLI、接続は別のリソースです。まず、CreateConnection API アクションを使用して接続を作成します。次に、CreateService API アクションを使用して、サービスの作成中に接続の ARN を指定します。

ソースディレクトリ

サービスを作成するときは、ソースディレクトリも指定します。デフォルトでは、App Runner はリポジトリのルートディレクトリをソースディレクトリとして使用します。ソースディレクトリは、アプリケーションのソースコードと設定ファイルを保存するソースコードリポジトリ内の場所です。ビルドコマンドと開始コマンドは、ソースディレクトリからも実行されます。App Runner API または を使用してサービス AWS CLI を作成または更新する場合は、CreateService および UpdateService API アクションでソースディレクトリを指定します。詳細については、次の「ソースディレクトリ」セクションを参照してください。

App Runner サービスの作成の詳細については、「」を参照してくださいthe section called “作成”。App Runner 接続の詳細については、「」を参照してくださいthe section called “Connections”。

ソースディレクトリ

App Runner サービスを作成するときは、リポジトリとブランチとともにソースディレクトリを指定できます。Source ディレクトリフィールドの値を、アプリケーションのソースコードと設定ファイルを保存するリポジトリディレクトリパスに設定します。App Runner は、指定したソースディレクトリパスからビルドコマンドとスタートコマンドを実行します。

ルートリポジトリディレクトリからソースディレクトリパスの値を絶対として入力します。値を指定しない場合、デフォルトでリポジトリの最上位ディレクトリになります。これはリポジトリルートディレクトリとも呼ばれます。

また、最上位リポジトリディレクトリの他に異なるソースディレクトリパスを指定することもできます。これにより、モノレポリポジトリアーキテクチャがサポートされます。つまり、複数のアプリケーションのソースコードは 1 つのリポジトリに保存されます。単一のモノレポから複数の App Runner サービスを作成してサポートするには、各サービスを作成するときに異なるソースディレクトリを指定します。

> **Note**
>
> 複数の App Runner サービスに同じソースディレクトリを指定すると、両方のサービスが個別にデプロイおよび動作します。

`apprunner.yaml` 設定ファイルを使用してサービスパラメータを定義する場合は、リポジトリのソースディレクトリフォルダに配置します。

デプロイトリガーオプションが自動に設定されている場合、ソースディレクトリでコミットした変更は自動デプロイをトリガーします。ソースディレクトリパスの変更のみが自動デプロイをトリガーします。ソースディレクトリの場所が自動デプロイの範囲にどのように影響するかを理解することが重要です。詳細については、「」の「自動デプロイ」を参照してくださいデプロイ方法。

> **Note**
>
> App Runner サービスが PHP マネージドランタイムを使用していて、デフォルトのルートリポジトリ以外のソースディレクトリを指定する場合は、正しい PHP ランタイムバージョンを使用することが重要です。詳細については、「PHP プラットフォームを使用する」を参照してください。

App Runner マネージドプラットフォーム

App Runner マネージドプラットフォームは、さまざまなプログラミング環境にマネージドランタイムを提供します。各マネージドランタイムを使用すると、プログラミング言語またはランタイム環境のバージョンに基づいてコンテナを簡単に構築して実行できます。マネージドランタイムを使用すると、App Runner はマネージドランタイムイメージで始まります。このイメージは Amazon Linux Docker イメージに基づいており、言語ランタイムパッケージ、いくつかのツール、一般的な依存関係パッケージが含まれています。App Runner は、このマネージドランタイムイメージをベースイメージとして使用し、アプリケーションコードを追加して Docker イメージを構築します。次に、このイメージをデプロイして、コンテナでウェブサービスを実行します。

App Runner コンソールまたは CreateService API オペレーションを使用してサービスを作成するときに、App Runner サービスのランタイムを指定します。ソースコードの一部としてランタイムを指定することもできます。コードリポジトリに含める App Runner 設定ファイルで `runtime`キーワードを使用します。マネージドランタイムの命名規則は *`<language-name><major-version>`* です。

App Runner は、デプロイまたはサービスの更新ごとに、サービスのランタイムを最新バージョンに更新します。アプリケーションで特定のバージョンのマネージドランタイムが必要な場合は、App Runner 設定ファイルの `runtime-version`キーワードを使用して指定できます。メジャーバージョンやマイナーバージョンなど、任意のレベルのバージョンにロックできます。App Runner は、サービスのランタイムに対して低レベルの更新のみを行います。

マネージドランタイムバージョンと App Runner ビルド

App Runner は、最新のメジャーバージョンランタイムで実行されるアプリケーション向けに更新されたビルドプロセスを提供します。この改訂されたビルドプロセスは、より高速で効率的です。また、アプリケーションの実行に必要なソースコード、ビルドアーティファクト、ランタイムのみを含む、フットプリントが小さい最終イメージを作成します。

新しいビルドプロセスを改訂された App Runner ビルドと呼び、元のビルドプロセスを元の App Runner ビルドと呼びます。以前のバージョンのランタイムプラットフォームへの重大な変更を避けるために、App Runner は改訂されたビルドを特定のランタイムバージョン、通常は新しくリリースされたメジャーリリースにのみ適用します。

`apprunner.yaml` 設定ファイルに新しいコンポーネントを導入し、改訂されたビルドを特定のユースケースに対して下位互換性を持たせ、アプリケーションのビルドをより柔軟に設定できるようにな

りました。これはオプションの`pre-run`パラメータです。以下のセクションでは、ビルドに関するその他の有用な情報とともに、このパラメータをいつ使用するかについて説明します。

次の表は、特定のマネージドランタイムバージョンに適用される App Runner ビルドのバージョンを示しています。このドキュメントは引き続き更新され、現在のランタイムについてお知らせします。

プラットフォーム	元のビルド	ビルドの改訂
Python – リリース情報	• Python 3.8 • Python 3.7	• Python 3.11 (!)
Node.js – リリース情報	• Node.js 16 • Node.js 14 • Node.js 12	• Node.js 22 • Node.js 18
Corretto – リリース情報	• Corretto 11 • Corretto 8	
.NET – リリース情報	• .NET 6	
PHP – リリース情報	• PHP 8.1	
Ruby – リリース情報	• Ruby 3.1	
Go – リリース情報	• Go 1	

> **Important**
>
> Python 3.11 – Python 3.11 マネージドランタイムを使用するサービスのビルド設定に関する具体的な推奨事項があります。詳細については、Python プラットフォームトピック特定のランタイムバージョンのコールアウトの「」を参照してください。

App Runner のビルドと移行の詳細

改訂されたビルドを使用する新しいランタイムにアプリケーションを移行する場合、ビルド設定を少し変更する必要がある場合があります。

移行に関する考慮事項のコンテキストを提供するために、最初に元の App Runner ビルドと改訂されたビルドの両方の高レベルプロセスについて説明します。次に、設定の更新が必要になる可能性のあるサービスに関する特定の属性について説明するセクションを示します。

元の App Runner ビルド

元の App Runner アプリケーションビルドプロセスは、 AWS CodeBuild サービスを活用します。初期ステップは、CodeBuild サービスによってキュレートされたイメージに基づいています。Docker ビルドプロセスは、該当する App Runner マネージドランタイムイメージをベースイメージとして使用するプロセスに従います。

一般的なステップは次のとおりです。

1. CodeBuild でキュレートされたイメージで`pre-build`コマンドを実行します。

   `pre-build` コマンドはオプションです。`apprunner.yaml` これらは設定ファイルでのみ指定できます。

2. 前のステップと同じイメージで CodeBuild を使用して`build`コマンドを実行します。

   `build` コマンドは必須です。これらは、App Runner コンソール、App Runner API、または`apprunner.yaml`設定ファイルで指定できます。

3. Docker ビルドを実行して、特定のプラットフォームとランタイムバージョンの App Runner マネージドランタイムイメージに基づいてイメージを生成します。

4. ステップ 2 で生成したイメージから `/app` ディレクトリをコピーします。送信先は、ステップ 3 で生成した App Runner マネージドランタイムイメージに基づくイメージです。

5. 生成された App Runner マネージドランタイムイメージで`build`コマンドを再度実行します。ビルドコマンドを再度実行して、ステップ 4 でコピーした`/app`ディレクトリのソースコードからビルドアーティファクトを生成します。このイメージは、後で App Runner によってデプロイされ、コンテナでウェブサービスを実行します。

   `build` コマンドは必須です。これらは、App Runner コンソール、App Runner API、または`apprunner.yaml`設定ファイルで指定できます。

6. ステップ 2 の CodeBuild イメージで`post-build`コマンドを実行します。

   `post-build` コマンドはオプションです。`apprunner.yaml` これらは設定ファイルでのみ指定できます。

ビルドが完了すると、App Runner はステップ 5 で生成された App Runner マネージドランタイムイメージをデプロイして、コンテナでウェブサービスを実行します。

改訂された App Runner ビルド

改訂されたビルドプロセスは、前のセクションで説明した元のビルドプロセスよりも高速で効率的です。これにより、以前のバージョンビルドで発生するビルドコマンドの重複がなくなります。また、ソースコード、ビルドアーティファクト、アプリケーションの実行に必要なランタイムのみを含む、フットプリントが小さい最終イメージを作成します。

このビルドプロセスでは、Docker マルチステージビルドを使用します。一般的なプロセスステップは次のとおりです。

1. ビルドステージ — App Runner ビルドイメージ上で `pre-build`および `build` コマンドを実行する docker ビルドプロセスを開始します。
   a. アプリケーションのソースコードを `/app` ディレクトリにコピーします。

      > **Note**
      > この`/app`ディレクトリは、Docker ビルドのすべてのステージで作業ディレクトリとして指定されます。

   b. `pre-build` コマンドを実行します。

      コマンドは`pre-build`オプションです。`apprunner.yaml` これらは設定ファイルでのみ指定できます。

   c. `build` コマンドを実行します。

      `build` コマンドは必須です。これらは、App Runner コンソール、App Runner API、または`apprunner.yaml`設定ファイルで指定できます。
2. パッケージングステージ — App Runner 実行イメージにも基づいている、最終的な顧客コンテナイメージを生成します。
   a. ディレクトリを以前のビルドステージ`/app`から新しい実行イメージにコピーします。これには、アプリケーションのソースコードと、前のステージのビルドアーティファクトが含まれます。
   b. `pre-run` コマンドを実行します。`build` コマンドを使用して`/app`ディレクトリの外部でランタイムイメージを変更する必要がある場合は、`apprunner.yaml`設定ファイルのこのセグメントに同じコマンドまたは必要なコマンドを追加します。

これは、改訂された App Runner ビルドをサポートするために導入された新しいパラメータです。

`pre-run` コマンドはオプションです。`apprunner.yaml` これらは設定ファイルでのみ指定できます。

> **メモ**
>
> - `pre-run` コマンドは、改訂されたビルドでのみサポートされます。サービスが元のビルドを使用するランタイムバージョンを使用している場合は、設定ファイルに追加しないでください。
> - `build` コマンドを使用して`/app`ディレクトリの外部を変更する必要がない場合は、`pre-run`コマンドを指定する必要はありません。

3. ビルド後ステージ — このステージはビルドステージから再開し、`post-build`コマンドを実行します。

   a. `/app` ディレクトリ内で`post-build`コマンドを実行します。

      `post-build` コマンドはオプションです。`apprunner.yaml` これらは設定ファイルでのみ指定できます。

ビルドが完了すると、App Runner は Run イメージをデプロイしてウェブサービスをコンテナで実行します。

> **Note**
>
> ビルドプロセスを設定する`apprunner.yaml`ときに、 の実行セクションの`env`エントリに誤解しないでください。ステップ 2 (b) で参照される `pre-run` コマンドパラメータは Run セクションにありますが、Run セクションの `env`パラメータを使用してビルドを設定しないでください。`pre-run` コマンドは、設定ファイルのビルドセクションで定義されている`env`変数のみを参照します。詳細については、App Runner 設定ファイルの章実行セクションの「」を参照してください。

移行に関する考慮事項のサービス要件

アプリケーション環境にこれら 2 つの要件のいずれかがある場合は、 `pre-run` コマンドを追加してビルド設定を修正する必要があります。

- `build` コマンドを使用して`/app`ディレクトリの外部を変更する必要がある場合。
- 必要な環境を作成するために`build`コマンドを 2 回実行する必要がある場合。これは非常にまれな要件です。ほとんどのビルドはこれを行いません。

`/app` ディレクトリ外の変更

- 改訂された App Runner ビルドでは、アプリケーションに `/app` ディレクトリ外の依存関係がないことを前提としています。
- `apprunner.yaml` ファイル、App Runner API、または App Runner コンソールで指定するコマンドは、 `/app` ディレクトリにビルドアーティファクトを生成する必要があります。
- `pre-build`、、および `post-build` コマンドを変更して`build`、すべてのビルドアーティファクトが `/app` ディレクトリにあることを確認できます。
- アプリケーションのビルドで、 サービスの生成されたイメージを `/app` ディレクトリの外部でさらに変更する必要がある場合は、 の新しい`pre-run`コマンドを使用できます`apprunner.yaml`。詳細については、「設定ファイルを使用した App Runner サービスオプションの設定」を参照してください。

`build` コマンドを 2 回実行する

- 元の App Runner ビルドは、最初にステップ 2、次にステップ 5 で`build`コマンドを 2 回実行します。 改訂された App Runner ビルドは、この冗長性を修復し、`build`コマンドを 1 回だけ実行します。アプリケーションに`build`コマンドを 2 回実行するための異常な要件がある場合、改訂された App Runner ビルドには、 `pre-run`パラメータを使用して同じコマンドを再度指定して実行するオプションが用意されています。これにより、同じダブルビルド動作が保持されます。

Python プラットフォームを使用する

Python AWS App Runner プラットフォームはマネージドランタイムを提供します。各ランタイムにより、Python バージョンに基づいてウェブアプリケーションを使用してコンテナを簡単に構築して実行できます。Python ランタイムを使用すると、App Runner はマネージド Python ランタイムイメージで始まります。このイメージは Amazon Linux Docker イメージに基づいており、Python の

バージョン用のランタイムパッケージと、いくつかのツールと一般的な依存関係パッケージが含まれています。App Runner は、このマネージドランタイムイメージをベースイメージとして使用し、アプリケーションコードを追加して Docker イメージを構築します。次に、このイメージをデプロイして、コンテナでウェブサービスを実行します。

App Runner コンソールまたは CreateService API オペレーションを使用してサービスを作成するときに、App Runner サービスのランタイムを指定します。ソースコードの一部としてランタイムを指定することもできます。コードリポジトリに含める App Runner 設定ファイルの `runtime`キーワードを使用します。マネージドランタイムの命名規則は *`<language-name><major-version>`* です。

有効な Python ランタイム名とバージョンについては、「」を参照してくださいthe section called “リリース情報”。

App Runner は、デプロイまたはサービスの更新ごとに、サービスのランタイムを最新バージョンに更新します。アプリケーションで特定のバージョンのマネージドランタイムが必要な場合は、App Runner 設定ファイルの `runtime-version`キーワードを使用して指定できます。メジャーバージョンやマイナーバージョンなど、任意のレベルのバージョンにロックできます。App Runner は、サービスのランタイムに対して低レベルの更新のみを行います。

Python ランタイムのバージョン構文: *`major`*`[.`*`minor`*`[.`*`patch`*`]]`

例: `3.8.5`

次の例は、バージョンロックを示しています。

- `3.8` – メジャーバージョンとマイナーバージョンをロックします。App Runner はパッチバージョンのみを更新します。
- `3.8.5` – 特定のパッチバージョンにロックします。App Runner はランタイムバージョンを更新しません。

トピック

- Python ランタイム設定
- 特定のランタイムバージョンのコールアウト
- Python ランタイムの例
- Python ランタイムリリース情報

Python ランタイム設定

マネージドランタイムを選択するときは、少なくとも コマンドを構築して実行することも設定する必要があります。App Runner サービスを作成または更新するときに設定します。これを行うには、次のいずれかの方法を使用します。

- App Runner コンソールの使用 – 作成プロセスまたは設定タブのビルドの設定セクションでコマンドを指定します。
- App Runner API の使用 – CreateService または UpdateService API オペレーションを呼び出します。CodeConfigurationValues データ型の `BuildCommand`および `StartCommand`メンバーを使用してコマンドを指定します。
- 設定ファイルの使用 – 最大 3 つのビルドフェーズで 1 つ以上のビルドコマンドと、アプリケーションを起動するための 1 つの実行コマンドを指定します。追加のオプションの設定があります。

設定ファイルの提供はオプションです。コンソールまたは API を使用して App Runner サービスを作成する場合、App Runner が作成時に設定を直接取得するか、設定ファイルから取得するかを指定します。

特定のランタイムバージョンのコールアウト

> **Note**
>
> App Runner は、Python 3.11、Node.js 22、Node.js 18 のランタイムバージョンに基づいて、アプリケーションの更新されたビルドプロセスを実行するようになりました。アプリケーションがこれらのランタイムバージョンのいずれかで実行されている場合、改訂されたビルドプロセスマネージドランタイムバージョンと App Runner ビルドの詳細については、「」を参照してください。他のすべてのランタイムバージョンを使用するアプリケーションは影響を受けず、元のビルドプロセスを引き続き使用します。

Python 3.11 (App Runner ビルドの改訂)

マネージド Python 3.11 ランタイムには、apprunner.yaml で次の設定を使用します。

- トップセクションの `runtime` キーを に設定します。 `python311`

Example

```
runtime: python311
```

- 依存関係をインストールするpipには、 pip3の代わりに を使用します。
- の代わりにpython3インタープリタを使用しますpython。
- pip3 インストーラをpre-runコマンドとして実行します。Python は/app、 ディレクトリの外部に依存関係をインストールします。App Runner は Python 3.11 用に改訂された App Runner ビルドを実行するため、apprunner.yamlファイルのビルドセクションのコマンドを使用して/appディレクトリの外部にインストールされたものはすべて失われます。詳細については、「改訂された App Runner ビルド」を参照してください。

Example

```
run:
  runtime-version: 3.11
  pre-run:
    - pip3 install pipenv
    - pipenv install
    - python3 copy-global-files.py
  command: pipenv run gunicorn django_apprunner.wsgi --log-file -
```

詳細については、このトピックの後半にある Python 3.11 用の拡張設定ファイルの例も参照してください。

Python ランタイムの例

次の例は、Python サービスを構築および実行するための App Runner 設定ファイルを示しています。最後の例は、Python ランタイムサービスにデプロイできる完全な Python アプリケーションのソースコードです。

> **Note**
>
> これらの例で使用されるランタイムバージョンは *3.7.7* および *3.11* です。使用するバージョンに置き換えることができます。サポートされている最新の Python ランタイムバージョンについては、「」を参照してくださいthe section called “リリース情報”。

最小 Python 設定ファイル

この例では、Python マネージドランタイムで使用できる最小限の設定ファイルを示しています。App Runner が最小限の設定ファイルで行う前提については、「」を参照してくださいthe section called “設定ファイルの例”。

Python 3.11 では、 コマンドpip3と python3 コマンドを使用します。詳細については、このトピックの後半にある Python 3.11 用の拡張設定ファイルの例を参照してください。

Example apprunner.yaml

```
version: 1.0
runtime: python3
build:
  commands:
    build:
      - pip install pipenv
      - pipenv install
run:
  command: python app.py
```

拡張 Python 設定ファイル

この例では、Python マネージドランタイムですべての設定キーを使用する方法を示します。

> **Note**
>
> これらの例で使用されるランタイムバージョンは *3.7.7* です。使用するバージョンに置き換えることができます。サポートされている最新の Python ランタイムバージョンについては、「」を参照してくださいthe section called “リリース情報”。
> Python 3.11 では、 コマンドpip3と python3 コマンドを使用します。詳細については、このトピックの後半にある Python 3.11 用の拡張設定ファイルの例を参照してください。

Example apprunner.yaml

```
version: 1.0
runtime: python3
build:
  commands:
```

```
    pre-build:
      - wget -c https://s3.amazonaws.com/amzn-s3-demo-bucket/test-lib.tar.gz -O - | tar
 -xz
    build:
      - pip install pipenv
      - pipenv install
    post-build:
      - python manage.py test
  env:
    - name: DJANGO_SETTINGS_MODULE
      value: "django_apprunner.settings"
    - name: MY_VAR_EXAMPLE
      value: "example"
run:
  runtime-version: 3.7.7
  command: pipenv run gunicorn django_apprunner.wsgi --log-file -
  network:
    port: 8000
    env: MY_APP_PORT
  env:
    - name: MY_VAR_EXAMPLE
      value: "example"
  secrets:
    - name: my-secret
      value-from: "arn:aws:secretsmanager:us-
east-1:123456789012:secret:testingstackAppRunnerConstr-kJFXde2ULKbT-S7t8xR:username::"
    - name: my-parameter
      value-from: "arn:aws:ssm:us-east-1:123456789012:parameter/parameter-name"
    - name: my-parameter-only-name
      value-from: "parameter-name"
```

拡張 Python 設定ファイル — Python 3.11 (改訂されたビルドを使用)

この例では、 で Python 3.11 マネージドランタイムを使用するすべての設定キーの使用を示しています`apprunner.yaml`。この例では、このバージョンの Python は改訂された App Runner ビルドを使用するため、 `pre-run`セクションが含まれています。

`pre-run` パラメータは、改訂された App Runner ビルドでのみサポートされます。アプリケーションが元の App Runner ビルドでサポートされているランタイムバージョンを使用している場合は、このパラメータを設定ファイルに挿入しないでください。詳細については、「マネージドランタイムバージョンと App Runner ビルド」を参照してください。

> **Note**
>
> これらの例で使用されるランタイムバージョンは *3.11* です。使用するバージョンに置き換えることができます。サポートされている最新の Python ランタイムバージョンについては、「」を参照してくださいthe section called “リリース情報”。

Example apprunner.yaml

```
version: 1.0
runtime: python311
build:
  commands:
    pre-build:
      - wget -c https://s3.amazonaws.com/amzn-s3-demo-bucket/test-lib.tar.gz -O - | tar
 -xz
    build:
      - pip3 install pipenv
      - pipenv install
    post-build:
      - python3 manage.py test
  env:
    - name: DJANGO_SETTINGS_MODULE
      value: "django_apprunner.settings"
    - name: MY_VAR_EXAMPLE
      value: "example"
run:
  runtime-version: 3.11
  pre-run:
    - pip3 install pipenv
    - pipenv install
    - python3 copy-global-files.py
  command: pipenv run gunicorn django_apprunner.wsgi --log-file -
  network:
    port: 8000
    env: MY_APP_PORT
  env:
    - name: MY_VAR_EXAMPLE
      value: "example"
  secrets:
    - name: my-secret
```

```
      value-from: "arn:aws:secretsmanager:us-
east-1:123456789012:secret:testingstackAppRunnerConstr-kJFXde2ULKbT-S7t8xR:username::"
    - name: my-parameter
      value-from: "arn:aws:ssm:us-east-1:123456789012:parameter/parameter-name"
    - name: my-parameter-only-name
      value-from: "parameter-name"
```

完全な Python アプリケーションソース

この例では、Python ランタイムサービスにデプロイできる完全な Python アプリケーションのソースコードを示します。

Example requirements.txt

```
pyramid==2.0
```

Example server.py

```
from wsgiref.simple_server import make_server
from pyramid.config import Configurator
from pyramid.response import Response
import os

def hello_world(request):
    name = os.environ.get('NAME')
    if name == None or len(name) == 0:
        name = "world"
    message = "Hello, " + name + "!\n"
    return Response(message)

if __name__ == '__main__':
    port = int(os.environ.get("PORT"))
    with Configurator() as config:
        config.add_route('hello', '/')
        config.add_view(hello_world, route_name='hello')
        app = config.make_wsgi_app()
    server = make_server('0.0.0.0', port, app)
    server.serve_forever()
```

Example apprunner.yaml

```
version: 1.0
```

```
runtime: python3
build:
  commands:
    build:
      - pip install -r requirements.txt
run:
  command: python server.py
```

Python ランタイムリリース情報

このトピックでは、App Runner がサポートする Python ランタイムバージョンの詳細を一覧表示します。

サポートされているランタイムバージョン — App Runner ビルドの改訂

ランタイム名	マイナーバージョン	含まれるパッケージ
Python 3.11 (Python311)	3.11.12	SQLite 3.50.0
	3.11.11	SQLite 3.49.1
	3.11.10	SQLite 3.46.1
	3.11.9	SQLite 3.46.1
	3.11.8	SQLite 3.45.2
	3.11.7	SQLite 3.44.2

メモ

- Python 3.11 – Python 3.11 マネージドランタイムを使用するサービスのビルド設定に関する具体的な推奨事項があります。詳細については、Python プラットフォームトピック特定のランタイムバージョンのコールアウトの「」を参照してください。
- App Runner は、最近リリースされた特定のメジャーランタイムのビルドプロセスを改訂しました。このため、このドキュメントの特定のセクションに、改訂された App Runner ビルドと元の App Runner ビルドへの参照が表示されます。詳細については、「マネージドランタイムバージョンと App Runner ビルド」を参照してください。

サポートされているランタイムバージョン — 元の App Runner ビルド

ランタイム名	マイナーバージョン	含まれているパッケージ
Python 3 (python3)	3.8.20	SQLite 3.50.0
	3.8.16	SQLite 3.46.1
	3.8.15	SQLite 3.40.0
	3.7.16	SQLite 3.50.0
	3.7.15	SQLite 3.40.0
	3.7.10	SQLite 3.40.0

> **Note**
>
> App Runner は、最近リリースされた特定のメジャーランタイムのビルドプロセスを改訂しました。このため、このドキュメントの特定のセクションには、改訂された App Runner ビルドと元の App Runner ビルドへの参照が表示されます。詳細については、「マネージドランタイムバージョンと App Runner ビルド」を参照してください。

Node.js プラットフォームを使用する

AWS App Runner Node.js プラットフォームはマネージドランタイムを提供します。各ランタイムにより、Node.js バージョンに基づいてウェブアプリケーションを使用してコンテナを簡単に構築および実行できます。Node.js ランタイムを使用すると、App Runner はマネージド Node.js ランタイムイメージで始まります。このイメージは Amazon Linux Docker イメージに基づいており、Node.js のバージョンと一部のツールのランタイムパッケージが含まれています。App Runner は、このマネージドランタイムイメージをベースイメージとして使用し、アプリケーションコードを追加して Docker イメージを構築します。次に、このイメージをデプロイして、コンテナでウェブサービスを実行します。

App Runner コンソールまたは CreateService API オペレーションを使用してサービスを作成するときに、App Runner サービスのランタイムを指定します。ソースコードの一部としてランタイムを指定することもできます。コードリポジトリに含める App Runner 設定ファイルで `runtime`キーワー

ドを使用します。マネージドランタイムの命名規則は *<language-name><major-version>* です。

有効な Node.js ランタイム名とバージョンについては、「」を参照してくださいthe section called "リリース情報"。

App Runner は、デプロイまたはサービスの更新ごとに、サービスのランタイムを最新バージョンに更新します。アプリケーションで特定のバージョンのマネージドランタイムが必要な場合は、App Runner 設定ファイルの `runtime-version`キーワードを使用して指定できます。メジャーバージョンやマイナーバージョンなど、任意のレベルのバージョンにロックできます。App Runner は、サービスのランタイムに対して低レベルの更新のみを行います。

Node.js ランタイムのバージョン構文: *major*[.*minor*[.*patch*]]

例: `22.14.0`

次の例は、バージョンロックを示しています。

- `22.14` – メジャーバージョンとマイナーバージョンをロックします。App Runner はパッチバージョンのみを更新します。
- `22.14.0` – 特定のパッチバージョンにロックします。App Runner はランタイムバージョンを更新しません。

トピック

- Node.js ランタイム設定
- 特定のランタイムバージョンのコールアウト
- Node.js ランタイムの例
- Node.js ランタイムリリース情報

Node.js ランタイム設定

マネージドランタイムを選択するときは、少なくとも コマンドを構築して実行することも設定する必要があります。App Runner サービスを作成または更新するときに設定します。これを行うには、次のいずれかの方法を使用します。

- App Runner コンソールの使用 – 作成プロセスまたは設定タブのビルドの設定セクションでコマンドを指定します。

- App Runner API の使用 – CreateService または UpdateService API オペレーションを呼び出します。CodeConfigurationValues データ型の `BuildCommand`および `StartCommand`メンバーを使用してコマンドを指定します。
- 設定ファイルの使用 – 最大 3 つのビルドフェーズで 1 つ以上のビルドコマンドと、アプリケーションを起動する 1 つの実行コマンドを指定します。追加のオプションの設定があります。

設定ファイルの提供はオプションです。コンソールまたは API を使用して App Runner サービスを作成する場合、App Runner が作成時に設定を直接取得するか、設定ファイルから取得するかを指定します。

Node.js ランタイムでは、ソースリポジトリのルート`package.json`にある という名前の JSON ファイルを使用してビルドとランタイムを設定することもできます。このファイルを使用して、Node.js エンジンのバージョン、依存関係パッケージ、およびさまざまなコマンド (コマンドラインアプリケーション) を設定できます。npm や yarn などのパッケージマネージャーは、このファイルをコマンドの入力として解釈します。

例：

- npm install は、 の `dependencies`および `devDependencies`ノードで定義されたパッケージをインストールします`package.json`。
- npm start または は、 の`scripts/start`ノードで定義されたコマンドnpm run startを実行します`package.json`。

次は、`package.json` ファイルの例です。

package.json

```
{
  "name": "node-js-getting-started",
  "version": "0.3.0",
  "description": "A sample Node.js app using Express 4",
  "engines": {
    "node": "22.14.0"
  },
  "scripts": {
    "start": "node index.js",
    "test": "node test.js"
  },
  "dependencies": {
```

```
    "cool-ascii-faces": "^1.3.4",
    "ejs": "^2.5.6",
    "express": "^4.15.2"
  },
  "devDependencies": {
    "got": "^11.3.0",
    "tape": "^4.7.0"
  }
}
```

の詳細についてはpackage.json、npm Docs ウェブサイトの package.json ファイルの作成を参照してください。

ヒント

- package.json ファイルがstartコマンドを定義する場合は、次の例に示すように、App Runner 設定ファイルのrunコマンドとして使用できます。

  Example

  package.json

  ```
  {
    "scripts": {
      "start": "node index.js"
    }
  }
  ```

  apprunner.yaml

  ```
  run:
    command: npm start
  ```

- 開発環境で を実行するnpm installと、npm はファイル を作成しますpackage-lock.json。このファイルには、インストールしたばかりのパッケージバージョンのスナップショットが含まれています。その後、npm が依存関係をインストールすると、これらの正確なバージョンが使用されます。yarn をインストールすると、 yarn.lock ファイルが作成されます。これらのファイルをソースコードリポジトリにコミットして、アプリケーションが開発してテストした依存関係のバージョンでインストールされていることを確認します。

- App Runner 設定ファイルを使用して Node.js バージョンを設定し、コマンドを開始することもできます。これを行うと、これらの定義は の定義よりも優先されますpackage.json。node のバージョンpackage.jsonと App Runner 設定ファイルruntime-versionの値の間に競合があると、App Runner ビルドフェーズが失敗します。

特定のランタイムバージョンのコールアウト

Node.js 22 および Node.js 18 (App Runner ビルドの改訂)

App Runner は、Python 3.11、Node.js 22、Node.js 18 のランタイムバージョンに基づいて、アプリケーションの更新されたビルドプロセスを実行するようになりました。アプリケーションがこれらのランタイムバージョンのいずれかで実行されている場合、改訂されたビルドプロセスマネージドランタイムバージョンと App Runner ビルドの詳細については、「」を参照してください。他のすべてのランタイムバージョンを使用するアプリケーションは影響を受けず、元のビルドプロセスを引き続き使用します。

Node.js ランタイムの例

次の例は、Node.js サービスを構築および実行するための App Runner 設定ファイルを示しています。

> **Note**
>
> これらの例で使用されるランタイムバージョンは *22.14.0* です。使用するバージョンに置き換えることができます。サポートされている最新の Node.js ランタイムバージョンについては、「」を参照してくださいthe section called “リリース情報”。

最小 Node.js 設定ファイル

この例では、Node.js マネージドランタイムで使用できる最小限の設定ファイルを示しています。App Runner が最小限の設定ファイルで実行する前提については、「」を参照してくださいthe section called “設定ファイルの例”。

Example apprunner.yaml

```
version: 1.0
```

```
runtime: nodejs22
build:
  commands:
    build:
      - npm install --production
run:
  command: node app.js
```

拡張 Node.js 設定ファイル

この例では、Node.js マネージドランタイムですべての設定キーを使用する方法を示します。

> **Note**
>
> これらの例で使用されるランタイムバージョンは *22.14.0* です。使用するバージョンに置き換えることができます。サポートされている最新の Node.js ランタイムバージョンについては、「」を参照してくださいthe section called “リリース情報”。

Example apprunner.yaml

```
version: 1.0
runtime: nodejs22
build:
  commands:
    pre-build:
      - npm install --only=dev
      - node test.js
    build:
      - npm install --production
    post-build:
      - node node_modules/ejs/postinstall.js
  env:
    - name: MY_VAR_EXAMPLE
      value: "example"
run:
  runtime-version: 22.14.0
  command: node app.js
  network:
    port: 8000
    env: APP_PORT
  env:
```

```
    - name: MY_VAR_EXAMPLE
      value: "example"
```

拡張 Node.js 設定ファイル – Node.js 22 (改訂されたビルドを使用)

この例では、 で Node.js マネージドランタイムを使用するすべての設定キーの使用を示しています`apprunner.yaml`。この例では、このバージョンの Node.js は改訂された App Runner ビルドを使用するため、 `pre-run`セクションが含まれています。

`pre-run` パラメータは、改訂された App Runner ビルドでのみサポートされます。アプリケーションが元の App Runner ビルドでサポートされているランタイムバージョンを使用している場合は、このパラメータを設定ファイルに挿入しないでください。詳細については、「マネージドランタイムバージョンと App Runner ビルド」を参照してください。

> **Note**
>
> これらの例で使用されるランタイムバージョンは *`22.14.0`* です。使用するバージョンに置き換えることができます。サポートされている最新の Node.js ランタイムバージョンについては、「」を参照してくださいthe section called “リリース情報”。

Example apprunner.yaml

```
version: 1.0
runtime: nodejs22
build:
  commands:
    pre-build:
      - npm install --only=dev
      - node test.js
    build:
      - npm install --production
    post-build:
      - node node_modules/ejs/postinstall.js
  env:
    - name: MY_VAR_EXAMPLE
      value: "example"
run:
  runtime-version: 22.14.0
  pre-run:
    - node copy-global-files.js
```

```
  command: node app.js
  network:
    port: 8000
    env: APP_PORT
  env:
    - name: MY_VAR_EXAMPLE
      value: "example"
```

Grunt を使用した Node.js アプリ

この例では、Grunt で開発された Node.js アプリケーションを設定する方法を示します。Grunt はコマンドライン JavaScript タスクランナーです。反復タスクを実行し、プロセスの自動化を管理して、人為的ミスを減らします。Grunt プラグインと Grunt プラグインは、npm を使用してインストールおよび管理されます。Grunt を設定するには、ソースリポジトリのルートに `Gruntfile.js` ファイルを含めます。

Example package.json

```
{
  "scripts": {
    "build": "grunt uglify",
    "start": "node app.js"
  },
  "devDependencies": {
    "grunt": "~0.4.5",
    "grunt-contrib-jshint": "~0.10.0",
    "grunt-contrib-nodeunit": "~0.4.1",
    "grunt-contrib-uglify": "~0.5.0"
  },
  "dependencies": {
    "express": "^4.15.2"
  },
}
```

Example Gruntfile.js

```
module.exports = function(grunt) {

  // Project configuration.
  grunt.initConfig({
    pkg: grunt.file.readJSON('package.json'),
    uglify: {
```

```
      options: {
        banner: '/*! <%= pkg.name %> <%= grunt.template.today("yyyy-mm-dd") %> */\n'
      },
      build: {
        src: 'src/<%= pkg.name %>.js',
        dest: 'build/<%= pkg.name %>.min.js'
      }
    }
  });

  // Load the plugin that provides the "uglify" task.
  grunt.loadNpmTasks('grunt-contrib-uglify');

  // Default task(s).
  grunt.registerTask('default', ['uglify']);

};
```

Example apprunner.yaml

> **Note**
>
> これらの例で使用されるランタイムバージョンは *22.14.0* です。使用するバージョンに置き換えることができます。サポートされている最新の Node.js ランタイムバージョンについては、「」を参照してくださいthe section called “リリース情報”。

```
version: 1.0
runtime: nodejs22
build:
  commands:
    pre-build:
      - npm install grunt grunt-cli
      - npm install --only=dev
      - npm run build
    build:
      - npm install --production
run:
  runtime-version: 22.14.0
  command: node app.js
  network:
    port: 8000
```

```
    env: APP_PORT
```

Node.js ランタイムリリース情報

> **Note**
>
> App Runner の標準的な非推奨ポリシーは、ランタイムの主要コンポーネントがコミュニティ長期サポート (LTS) が終了し、セキュリティ更新プログラムが利用できなくなったときに、ランタイムを非推奨にすることです。場合によっては、App Runner は、ランタイムでサポートされている言語バージョンのend-of-supportを超えて、限られた期間ランタイムの非推奨化を遅らせることがあります。このようなケースの例としては、ランタイムのサポートを拡張して、お客様が移行の時間を確保できます。

このトピックでは、App Runner がサポートする Node.js ランタイムバージョンの詳細を一覧表示します。

サポートされているランタイムバージョン — App Runner ビルドの改訂

ランタイム名	マイナーバージョン	含まれるパッケージ
Node.js 22 (nodejs22)	22.16.0	npm 10.9.2、ヤーン 1.22.22
Node.js 22 (nodejs22)	22.14.0	npm 10.9.2、ヤーン 1.22.22

> **Note**
>
> App Runner は、最近リリースされた特定のメジャーランタイムに対して、改訂されたビルドプロセスを提供します。このため、このドキュメントの特定のセクションには、改訂された App Runner ビルドと元の App Runner ビルドへの参照が表示されます。詳細については、「マネージドランタイムバージョンと App Runner ビルド」を参照してください。

サポートされているランタイムバージョン — App Runner ビルドの改訂

ランタイム名	マイナーバージョン	含まれているパッケージ
Node.js 18 (nodejs18)	18.20.8	npm 10.8.2、ヤーン 1.22.22

ランタイム名	マイナーバージョン	含まれているパッケージ
	18.20.7	npm 10.8.2、ヤーン 1.22.22
	18.20.6	npm 10.8.2、ヤーン 1.22.22
	18.20.5	npm 10.8.2、ヤーン 1.22.22
	18.20.4	npm 10.7.0、ヤーン 1.22.22
	18.20.3	npm 10.7.0、ヤーン 1.22.22
	18.20.2	npm 10、ヤーン *
	18.19.1	npm 10、ヤーン *
	18.19.0	npm 10、ヤーン *

サポートされているランタイムバージョン — 元の App Runner ビルド

ランタイム名	マイナーバージョン	含まれているパッケージ
Node.js 16 (nodejs16)	16.20.2	npm 8.19.4、ヤーン 1.22.22
	16.20.1	npm 8.19.4、ヤーン *
	16.20.0	npm 8.19.4、ヤーン *
	16.19.1	npm 8.19.4、ヤーン *
	16.19.0	npm 8.19.4、ヤーン *
	16.18.1	npm 8.19.4、ヤーン *
	16.17.1	npm 8.19.4、ヤーン *
	16.17.0	npm 8.19.4、ヤーン *
Node.js 14 (nodejs14)	14.21.3	npm 6.14.18、ヤーン 1.22.22

ランタイム名	マイナーバージョン	含まれているパッケージ
	14.21.2	npm 6.14.18、 yarn *
	14.21.1	npm 6.14.18、 yarn *
	14.20.1	npm 6.14.18、 yarn *
	14.19.0	npm 6.14.18、 yarn *
Node.js 12 (nodejs12)	12.22.12	npm 6.14.16、ヤーン 1.22.22
	12.21.0	npm 6.14.16、 yarn *

Java プラットフォームの使用

Java AWS App Runner プラットフォームはマネージドランタイムを提供します。各ランタイムにより、Java バージョンに基づいてウェブアプリケーションを使用してコンテナを簡単に構築および実行できます。Java ランタイムを使用すると、App Runner はマネージド Java ランタイムイメージから開始します。このイメージは Amazon Linux Docker イメージに基づいており、Java のバージョンと一部のツール用のランタイムパッケージが含まれています。App Runner は、このマネージドランタイムイメージをベースイメージとして使用し、Docker イメージを構築するためのアプリケーションコードを追加します。次に、このイメージをデプロイして、コンテナでウェブサービスを実行します。

App Runner コンソールまたは CreateService API オペレーションを使用してサービスを作成するときに、App Runner サービスのランタイムを指定します。ソースコードの一部としてランタイムを指定することもできます。コードリポジトリに含める App Runner 設定ファイルで `runtime`キーワードを使用します。マネージドランタイムの命名規則は `<language-name><major-version>` です。

現時点では、サポートされているすべての Java ランタイムは Amazon Corretto に基づいています。有効な Java ランタイム名とバージョンについては、「」を参照してくださいthe section called “リリース情報”。

App Runner は、デプロイまたはサービスの更新のたびに、サービスのランタイムを最新バージョンに更新します。アプリケーションで特定のバージョンのマネージドランタイムが必要な場合は、App Runner 設定ファイルの `runtime-version`キーワードを使用して指定できます。メジャーバージョ

ンやマイナーバージョンなど、任意のレベルのバージョンにロックできます。App Runner は、サービスのランタイムに対してのみ低レベルの更新を行います。

Amazon Corretto ランタイムのバージョン構文：

ランタイム	[Syntax] (構文)	例
corretto11	`11.0[.openjdk-update [.openjdk-build [.corretto-specific-revision ]]]`	`11.0.13.08.1`
corretto8	`8[.openjdk-update [.openjdk-build [.corretto-specific-revision ]]]`	`8.312.07.1`

次の例は、バージョンロックを示しています。

- `11.0.13` – Open JDK 更新バージョンをロックします。App Runner は Open JDK と Amazon Corretto の下位レベルのビルドのみを更新します。
- `11.0.13.08.1` – 特定のバージョンにロックします。App Runner はランタイムバージョンを更新しません。

トピック

- Java ランタイム設定
- Java ランタイムの例
- Java ランタイムリリース情報

Java ランタイム設定

マネージドランタイムを選択するときは、少なくともコマンドを構築して実行するように設定する必要があります。App Runner サービスを作成または更新するときに設定します。これを行うには、次のいずれかの方法を使用します。

- App Runner コンソールの使用 – 作成プロセスまたは設定タブのビルドの設定セクションでコマンドを指定します。

- App Runner API の使用 – CreateService または UpdateService API オペレーションを呼び出します。CodeConfigurationValues データ型の `BuildCommand`および `StartCommand`メンバーを使用してコマンドを指定します。
- 設定ファイルの使用 – 最大 3 つのビルドフェーズで 1 つ以上のビルドコマンドと、アプリケーションを起動する 1 つの実行コマンドを指定します。追加のオプションの設定があります。

設定ファイルの提供はオプションです。コンソールまたは API を使用して App Runner サービスを作成する場合、App Runner が作成時に設定を直接取得するか、設定ファイルから取得するかを指定します。

Java ランタイムの例

次の例は、Java サービスを構築および実行するための App Runner 設定ファイルを示しています。最後の例は、Corretto 11 ランタイムサービスにデプロイできる完全な Java アプリケーションのソースコードです。

> **Note**
>
> これらの例で使用されるランタイムバージョンは *`11.0.13.08.1`* です。使用するバージョンに置き換えることができます。サポートされている最新の Java ランタイムバージョンについては、「」を参照してくださいthe section called “リリース情報”。

Corretto 11 の最小設定ファイル

この例では、Corretto 11 マネージドランタイムで使用できる最小限の設定ファイルを示しています。App Runner が最小限の設定ファイルで行う前提条件については、「」を参照してください。

Example apprunner.yaml

```
version: 1.0
runtime: corretto11
build:
  commands:
    build:
      - mvn clean package
run:
  command: java -Xms256m -jar target/MyApp-1.0-SNAPSHOT.jar .
```

拡張 Corretto 11 設定ファイル

この例では、Corretto 11 マネージドランタイムですべての設定キーを使用する方法を示します。

> **Note**
>
> これらの例で使用されるランタイムバージョンは *11.0.13.08.1* です。使用するバージョンに置き換えることができます。サポートされている最新の Java ランタイムバージョンについては、「」を参照してくださいthe section called “リリース情報”。

Example apprunner.yaml

```
version: 1.0
runtime: corretto11
build:
  commands:
    pre-build:
      - yum install some-package
      - scripts/prebuild.sh
    build:
      - mvn clean package
    post-build:
      - mvn clean test
  env:
    - name: M2
      value: "/usr/local/apache-maven/bin"
    - name: M2_HOME
      value: "/usr/local/apache-maven/bin"
run:
  runtime-version: 11.0.13.08.1
  command: java -Xms256m -jar target/MyApp-1.0-SNAPSHOT.jar .
  network:
    port: 8000
    env: APP_PORT
  env:
    - name: MY_VAR_EXAMPLE
      value: "example"
```

Corretto 11 アプリケーションソースを完了する

この例では、Corretto 11 ランタイムサービスにデプロイできる完全な Java アプリケーションのソースコードを示しています。

Example src/main/java/com/HelloWorld/HelloWorld.java

```
package com.HelloWorld;

import org.springframework.web.bind.annotation.RequestMapping;
import org.springframework.web.bind.annotation.RestController;

@RestController
public class HelloWorld {

    @RequestMapping("/")
    public String index(){
        String s = "Hello World";
        return s;
    }
}
```

Example src/main/java/com/HelloWorld/Main.java

```
package com.HelloWorld;

import org.springframework.boot.SpringApplication;
import org.springframework.boot.autoconfigure.SpringBootApplication;

@SpringBootApplication
public class Main {

    public static void main(String[] args) {

        SpringApplication.run(Main.class, args);
    }
}
```

Example apprunner.yaml

```
version: 1.0
runtime: corretto11
```

```
build:
  commands:
    build:
      - mvn clean package
run:
  command: java -Xms256m -jar target/HelloWorldJavaApp-1.0-SNAPSHOT.jar .
  network:
    port: 8080
```

Example pom.xml

```
<?xml version="1.0" encoding="UTF-8"?>
<project xmlns="http://maven.apache.org/POM/4.0.0"
     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
     xsi:schemaLocation="http://maven.apache.org/POM/4.0.0 http://maven.apache.org/xsd/
maven-4.0.0.xsd">
  <modelVersion>4.0.0</modelVersion>
  <parent>
    <groupId>org.springframework.boot</groupId>
    <artifactId>spring-boot-starter-parent</artifactId>
    <version>2.3.1.RELEASE</version>
    <relativePath/>
  </parent>
  <groupId>com.HelloWorld</groupId>
  <artifactId>HelloWorldJavaApp</artifactId>
  <version>1.0-SNAPSHOT</version>

  <properties>
    <java.version>11</java.version>
  </properties>

  <dependencies>
    <dependency>
      <groupId>org.springframework.boot</groupId>
      <artifactId>spring-boot-starter-data-rest</artifactId>
    </dependency>

    <dependency>
      <groupId>org.springframework.boot</groupId>
      <artifactId>spring-boot-starter-test</artifactId>
      <scope>test</scope>
      <exclusions>
        <exclusion>
```

```
          <groupId>org.junit.vintage</groupId>
          <artifactId>junit-vintage-engine</artifactId>
        </exclusion>
      </exclusions>
    </dependency>
  </dependencies>

  <build>
    <plugins>
      <plugin>
        <groupId>org.springframework.boot</groupId>
        <artifactId>spring-boot-maven-plugin</artifactId>
      </plugin>
      <plugin>
        <groupId>org.apache.maven.plugins</groupId>
        <artifactId>maven-compiler-plugin</artifactId>
        <version>3.8.0</version>
        <configuration>
          <release>11</release>
        </configuration>
      </plugin>
    </plugins>
  </build>
</project>
```

Java ランタイムリリース情報

このトピックでは、App Runner がサポートする Java ランタイムバージョンの詳細を一覧表示します。

サポートされているランタイムバージョン — 元の App Runner ビルド

ランタイム名	マイナーバージョン	含まれるパッケージ
Corretto 11 (corretto11)	11.0.27.6.1	Maven 3.9.9、Gradle 6.9.4
	11.0.26.4.1	Maven 3.9.9、Gradle 6.9.4
	11.0.25.9.1	Maven 3.9.9、Gradle 6.9.4
	11.0.24.8.1	Maven 3.9.9、Gradle 6.9.4
	11.0.23.9.1	Maven 3.9.8、Gradle 6.9.4

ランタイム名	マイナーバージョン	含まれるパッケージ
	11.0.22.7.1	Maven 3.9.6、Gradle 6.9.4
	11.0.21.9.1	Maven 3.9.6、Gradle 6.9.4
	11.0.21.9.1	Maven 3.9.5、Gradle 6.9.4
	11.0.20.8.1	Maven 3.9.3、Gradle 6.9.4
	11.0.19.7.1	Maven 3.9.3、Gradle 6.9.4
	11.0.18.10.1	Maven 3.9.1、Gradle 6.9.4
	11.0.17.8.1	Maven 3.8.6、Gradle 6.9.3
	11.0.16.9.1	Maven 3.8.6、Gradle 6.9.2
	11.0.13.08.1	Maven 3.6.3、Gradle 6.5
Corretto 8 (corretto8)	8.452.09.2	Maven 3.9.9、Gradle 6.9.4
	8.452.09.1	Maven 3.9.9、Gradle 6.9.4
	8.442.06.1	Maven 3.9.9、Gradle 6.9.4
	8.432.06.1	Maven 3.9.9、Gradle 6.9.4
	8.422.05.1	Maven 3.9.9、Gradle 6.9.4
	8.412.08.1	Maven 3.9.8、Gradle 6.9.4
	8.402.08.1	Maven 3.9.6、Gradle 6.9.4
	8.392.08.1	Maven 3.9.6、Gradle 6.9.4
	8.382.05.1	Maven 3.9.4、Gradle 6.9.4
	8.372.07.1	Maven 3.9.3、Gradle 6.9.4
	8.362.08.1	Maven 3.9.1、Gradle 6.9.4

ランタイム名	マイナーバージョン	含まれるパッケージ
	8.352.08.1	Maven 3.8.6、Gradle 6.9.3
	8.342.07.4	Maven 3.8.6、Gradle 6.9.2
	8.312.07.1	Maven 3.6.3、Gradle 6.5

> **Note**
>
> App Runner は、最近リリースされた特定のメジャーランタイムのビルドプロセスを改訂しました。このため、このドキュメントの特定のセクションに、改訂された App Runner ビルドと元の App Runner ビルドへの参照が表示されます。詳細については、「マネージドランタイムバージョンと App Runner ビルド」を参照してください。

.NET プラットフォームを使用する

AWS App Runner .NET プラットフォームはマネージドランタイムを提供します。各ランタイムにより、.NET バージョンに基づくウェブアプリケーションでコンテナを簡単に構築して実行できます。.NET ランタイムを使用すると、App Runner はマネージド .NET ランタイムイメージから開始します。このイメージは Amazon Linux Docker イメージに基づいており、.NET のバージョン用のランタイムパッケージと、いくつかのツールと一般的な依存関係パッケージが含まれています。App Runner は、このマネージドランタイムイメージをベースイメージとして使用し、アプリケーションコードを追加して Docker イメージを構築します。次に、このイメージをデプロイして、コンテナでウェブサービスを実行します。

App Runner コンソールまたは CreateService API オペレーションを使用してサービスを作成するときに、App Runner サービスのランタイムを指定します。ソースコードの一部としてランタイムを指定することもできます。コードリポジトリに含める App Runner 設定ファイルで `runtime`キーワードを使用します。マネージドランタイムの命名規則は *`<language-name><major-version>`* です。

有効な .NET ランタイム名とバージョンについては、「」を参照してくださいthe section called “リリース情報”。

App Runner は、デプロイまたはサービスの更新のたびに、サービスのランタイムを最新バージョンに更新します。アプリケーションで特定のバージョンのマネージドランタイムが必要な場合は、App

Runner 設定ファイルの `runtime-version`キーワードを使用して指定できます。メジャーバージョンやマイナーバージョンなど、任意のレベルのバージョンにロックできます。App Runner は、サービスのランタイムに対してのみ低レベルの更新を行います。

.NET ランタイムのバージョン構文: `major[.minor[.patch]]`

例: `6.0.9`

次の例は、バージョンロックを示しています。

- `6.0` – メジャーバージョンとマイナーバージョンをロックします。App Runner はパッチバージョンのみを更新します。
- `6.0.9` – 特定のパッチバージョンにロックします。App Runner はランタイムバージョンを更新しません。

トピック

- .NET ランタイム設定
- .NET ランタイムの例
- .NET ランタイムリリース情報

.NET ランタイム設定

マネージドランタイムを選択するときは、少なくとも コマンドを構築して実行するように設定する必要があります。App Runner サービスを作成または更新するときに設定します。これは、次のいずれかの方法を使用して実行できます。

- App Runner コンソールの使用 – 作成プロセスまたは設定タブのビルドの設定セクションでコマンドを指定します。
- App Runner API の使用 – CreateService または UpdateService API オペレーションを呼び出します。CodeConfigurationValues データ型の `BuildCommand`および `StartCommand`メンバーを使用してコマンドを指定します。
- 設定ファイルの使用 – 最大 3 つのビルドフェーズで 1 つ以上のビルドコマンドと、アプリケーションを起動する 1 つの実行コマンドを指定します。追加のオプションの設定があります。

設定ファイルの提供はオプションです。コンソールまたは API を使用して App Runner サービスを作成する場合、App Runner が作成時に設定を直接取得するか、設定ファイルから取得するかを指定します。

.NET ランタイムの例

次の例は、.NET サービスを構築および実行するための App Runner 設定ファイルを示しています。最後の例は、.NET ランタイムサービスにデプロイできる完全な .NET アプリケーションのソースコードです。

> **Note**
>
> これらの例で使用されるランタイムバージョンは `6.0.9` です。使用するバージョンに置き換えることができます。サポートされている最新の .NET ランタイムバージョンについては、「」を参照してくださいthe section called “リリース情報”。

最小 .NET 設定ファイル

この例では、.NET マネージドランタイムで使用できる最小限の設定ファイルを示しています。App Runner が最小限の設定ファイルで行う前提条件については、「」を参照してくださいthe section called “設定ファイルの例”。

Example apprunner.yaml

```
version: 1.0
runtime: dotnet6
build:
  commands:
    build:
      - dotnet publish -c Release -o out
run:
  command: dotnet out/HelloWorldDotNetApp.dll
```

拡張 .NET 設定ファイル

この例では、.NET マネージドランタイムですべての設定キーを使用する方法を示します。

> **Note**
>
> これらの例で使用されるランタイムバージョンは *6.0.9* です。使用するバージョンに置き換えることができます。サポートされている最新の .NET ランタイムバージョンについては、「」を参照してくださいthe section called “リリース情報”。

Example apprunner.yaml

```
version: 1.0
runtime: dotnet6
build:
  commands:
    pre-build:
      - scripts/prebuild.sh
    build:
      - dotnet publish -c Release -o out
    post-build:
      - scripts/postbuild.sh
  env:
    - name: MY_VAR_EXAMPLE
      value: "example"
run:
  runtime-version: 6.0.9
  command: dotnet out/HelloWorldDotNetApp.dll
  network:
    port: 5000
    env: APP_PORT
  env:
    - name: ASPNETCORE_URLS
      value: "http://*:5000"
```

完全な .NET アプリケーションソース

この例では、.NET ランタイムサービスにデプロイできる完全な .NET アプリケーションのソースコードを示します。

> **Note**
>
> - 次のコマンドを実行して、シンプルな .NET 6 ウェブアプリケーションを作成します。
> `dotnet new web --name HelloWorldDotNetApp -f net6.0`

- 作成した .NET 6 ウェブアプリ`apprunner.yaml`に を追加します。

Example HelloWorldDotNetApp

```
version: 1.0
runtime: dotnet6
build:
  commands:
    build:
      - dotnet publish -c Release -o out
run:
  command: dotnet out/HelloWorldDotNetApp.dll
  network:
    port: 5000
    env: APP_PORT
  env:
    - name: ASPNETCORE_URLS
      value: "http://*:5000"
```

.NET ランタイムリリース情報

このトピックでは、App Runner がサポートする .NET ランタイムバージョンの詳細を一覧表示します。

サポートされているランタイムバージョン — 元の App Runner ビルド

ランタイム名	マイナーバージョン	含まれるパッケージ
.NET 6 (dotnet6)	6.0.36	.NET SDK 6.0.428
	6.0.33	.NET SDK 6.0.425
	6.0.32	.NET SDK 6.0.424
	6.0.31	.NET SDK 6.0.423
	6.0.30	.NET SDK 6.0.422
	6.0.29	.NET SDK 6.0.421
	6.0.28	.NET SDK 6.0.420

ランタイム名	マイナーバージョン	含まれるパッケージ
	6.0.26	.NET SDK 6.0.418
	6.0.25	.NET SDK 6.0.417
	6.0.24	.NET SDK 6.0.416
	6.0.22	.NET SDK 6.0.414
	6.0.21	.NET SDK 6.0.413
	6.0.20	.NET SDK 6.0.412
	6.0.19	.NET SDK 6.0.411
	6.0.16	.NET SDK 6.0.408
	6.0.15	.NET SDK 6.0.407
	6.0.14	.NET SDK 6.0.406
	6.0.13	.NET SDK 6.0.405
	6.0.12	.NET SDK 6.0.404
	6.0.11	.NET SDK 6.0.403
	6.0.10	.NET SDK 6.0.402
	6.0.9	.NET SDK 6.0.401

> **Note**
>
> App Runner は、最近リリースされた特定のメジャーランタイムのビルドプロセスを改訂しました。このため、このドキュメントの特定のセクションには、改訂された App Runner ビルドと元の App Runner ビルドへの参照が表示されます。詳細については、「マネージドランタイムバージョンと App Runner ビルド」を参照してください。

PHP プラットフォームを使用する

AWS App Runner PHP プラットフォームはマネージドランタイムを提供します。各ランタイムを使用して、PHP バージョンに基づいてウェブアプリケーションでコンテナを構築および実行できます。PHP ランタイムを使用すると、App Runner はマネージド PHP ランタイムイメージから開始します。このイメージは Amazon Linux Docker イメージに基づいており、PHP のバージョンと一部のツール用のランタイムパッケージが含まれています。App Runner は、このマネージドランタイムイメージをベースイメージとして使用し、アプリケーションコードを追加して Docker イメージを構築します。次に、このイメージをデプロイして、コンテナでウェブサービスを実行します。

App Runner コンソールまたは CreateService API オペレーションを使用してサービスを作成するときに、App Runner サービスのランタイムを指定します。ソースコードの一部としてランタイムを指定することもできます。コードリポジトリに含める App Runner 設定ファイルで `runtime`キーワードを使用します。マネージドランタイムの命名規則は *`<language-name><major-version>`* です。

有効な PHP ランタイム名とバージョンについては、「」を参照してくださいthe section called “リリース情報”。

App Runner は、デプロイまたはサービスの更新ごとに、サービスのランタイムを最新バージョンに更新します。アプリケーションで特定のバージョンのマネージドランタイムが必要な場合は、App Runner 設定ファイルの `runtime-version`キーワードを使用して指定できます。メジャーバージョンやマイナーバージョンなど、任意のレベルのバージョンにロックできます。App Runner は、サービスのランタイムに対してのみ低レベルの更新を行います。

PHP ランタイムのバージョン構文: *`major`*`[.`*`minor`*`[.`*`patch`*`]]`

例: `8.1.10`

バージョンロックの例を次に示します。

- `8.1` – メジャーバージョンとマイナーバージョンをロックします。App Runner はパッチバージョンのみを更新します。
- `8.1.10` – 特定のパッチバージョンにロックします。App Runner はランタイムバージョンを更新しません。

> **Important**
>
> デフォルトのリポジトリルートディレクトリ以外の場所で App Runner サービスのコードリポジトリソースディレクトリを指定する場合は、PHP マネージドランタイムバージョンが PHP 8.1.22以降である必要があります。より前の PHP ランタイムバージョン8.1.22では、デフォルトのルートソースディレクトリのみを使用できます。

トピック

- PHP ランタイム設定
- 互換性
- PHP ランタイムの例
- PHP ランタイムリリース情報

PHP ランタイム設定

マネージドランタイムを選択するときは、少なくとも コマンドを構築して実行するように設定する必要があります。App Runner サービスを作成または更新するときに設定します。これを行うには、次のいずれかの方法を使用します。

- App Runner コンソールの使用 – 作成プロセスまたは設定タブのビルドの設定セクションでコマンドを指定します。
- App Runner API の使用 – CreateService または UpdateService API オペレーションを呼び出します。CodeConfigurationValues データ型の `BuildCommand`および `StartCommand`メンバーを使用してコマンドを指定します。
- 設定ファイルの使用 – 最大 3 つのビルドフェーズで 1 つ以上のビルドコマンドと、アプリケーションを起動する 1 つの実行コマンドを指定します。追加のオプションの設定があります。

設定ファイルの提供はオプションです。コンソールまたは API を使用して App Runner サービスを作成する場合、App Runner が作成時に設定を直接取得するか、設定ファイルから取得するかを指定します。

互換性

App Runner サービスは、次のいずれかのウェブサーバーを使用して PHP プラットフォームで実行できます。

- Apache HTTP Server
- NGINX

Apache HTTP Server および NGINXは PHP-FPM と互換性があります。Apache HTTP Server および は、次のいずれかNGINXを使用して開始できます。

- スーパーバイザー - の実行の詳細については、「スーパーバイザーの実行」を参照してください。supervisord
- 起動スクリプト

Apache HTTP Server または NGINX を使用して PHP プラットフォームで App Runner サービスを設定する方法の例については、「」を参照してくださいthe section called “完全な PHP アプリケーションソース”。

ファイル構造

は、ウェブサーバーの `root` ディレクトリの `public`フォルダにインストール`index.php`する必要があります。

> **Note**
>
> `startup.sh` または `supervisord.conf`ファイルは、ウェブサーバーのルートディレクトリに保存することをお勧めします。`start` コマンドが、 `startup.sh`または `supervisord.conf` ファイルが保存されている場所を指していることを確認します。

を使用している場合のファイル構造の例を次に示しますsupervisord。

```
/
## public/
#  ## index.php
## apprunner.yaml
## supervisord.conf
```

スタートアップスクリプトを使用している場合のファイル構造の例を次に示します。

```
/
```

```
## public/
#  ## index.php
## apprunner.yaml
## startup.sh
```

これらのファイル構造は、App Runner サービス用に指定されたコードリポジトリのソースディレクトリに保存することをお勧めします。

```
/<sourceDirectory>/
## public/
#  ## index.php
## apprunner.yaml
## startup.sh
```

> **Important**
>
> デフォルトのリポジトリルートディレクトリ以外の場所で App Runner サービスのコードリポジトリソースディレクトリを指定する場合は、PHP マネージドランタイムバージョンが PHP `8.1.22`以降である必要があります。より前の PHP ランタイムバージョン`8.1.22`では、デフォルトのルートソースディレクトリのみを使用できます。
> App Runner は、デプロイまたはサービスの更新ごとに、サービスのランタイムを最新バージョンに更新します。App Runner 設定ファイルの `runtime-version`キーワードを使用してバージョンロックを指定しない限り、サービスはデフォルトで最新のランタイムを使用します。

PHP ランタイムの例

PHP サービスの構築と実行に使用される App Runner 設定ファイルの例を次に示します。

最小 PHP 設定ファイル

次の例は、PHP マネージドランタイムで使用できる最小限の設定ファイルです。最小限の設定ファイルの詳細については、「」を参照してくださいthe section called “設定ファイルの例”。

Example apprunner.yaml

```
version: 1.0
runtime: php81
```

```
build:
  commands:
    build:
      - echo example build command for PHP
run:
  command: ./startup.sh
```

拡張 PHP 設定ファイル

次の例では、PHP マネージドランタイムですべての設定キーを使用します。

> **Note**
>
> これらの例で使用されるランタイムバージョンは *8.1.10* です。使用するバージョンに置き換えることができます。サポートされている最新の PHP ランタイムバージョンについては、「」を参照してくださいthe section called “リリース情報”。

Example apprunner.yaml

```
version: 1.0
runtime: php81
build:
  commands:
     pre-build:
      - scripts/prebuild.sh
    build:
      - echo example build command for PHP
    post-build:
      - scripts/postbuild.sh
  env:
    - name: MY_VAR_EXAMPLE
      value: "example"
run:
  runtime-version: 8.1.10
  command: ./startup.sh
  network:
    port: 5000
    env: APP_PORT
  env:
    - name: MY_VAR_EXAMPLE
      value: "example"
```

完全な PHP アプリケーションソース

次の例は、 Apache HTTP Serverまたは を使用して PHP ランタイムサービスにデプロイするために使用できる PHP アプリケーションのソースコードですNGINX。これらの例では、デフォルトのファイル構造を使用することを前提としています。

Apache HTTP Server を使用して で PHP プラットフォームを実行する supervisord

Example ファイル構造

> **Note**
>
> - `supervisord.conf` ファイルはリポジトリ内の任意の場所に保存できます。`start` コマンドが`supervisord.conf`ファイルの保存先を指していることを確認します。
> - は、 `root` ディレクトリの `public`フォルダにインストール`index.php`する必要があります。

```
/
## public/
#  ## index.php
## apprunner.yaml
## supervisord.conf
```

Example supervisord.conf

```
[supervisord]
nodaemon=true

[program:httpd]
command=httpd -DFOREGROUND
autostart=true
autorestart=true
stdout_logfile=/dev/stdout
stdout_logfile_maxbytes=0
stderr_logfile=/dev/stderr
stderr_logfile_maxbytes=0

[program:php-fpm]
command=php-fpm -F
autostart=true
```

```
autorestart=true
stdout_logfile=/dev/stdout
stdout_logfile_maxbytes=0
stderr_logfile=/dev/stderr
stderr_logfile_maxbytes=0
```

Example apprunner.yaml

```
version: 1.0
runtime: php81
build:
  commands:
    build:
      - PYTHON=python2 amazon-linux-extras install epel
      - yum -y install supervisor
run:
  command: supervisord
  network:
    port: 8080
    env: APP_PORT
```

Example index.php

```
<html>
<head> <title>First PHP App</title> </head>
<body>
<?php
    print("Hello World!");
    print("<br>");
?>
</body>
</html>
```

Apache HTTP Server を使用して で PHP プラットフォームを実行する startup script

Example ファイル構造

> **Note**
>
> - `startup.sh` ファイルはリポジトリ内の任意の場所に保存できます。`start` コマンドが`startup.sh`ファイルの保存先を指していることを確認します。

- は、 root ディレクトリの publicフォルダにインストールindex.phpする必要があります。

```
/
## public/
#  ## index.php
## apprunner.yaml
## startup.sh
```

Example startup.sh

```
#!/bin/bash

set -o monitor

trap exit SIGCHLD

# Start apache
httpd -DFOREGROUND &

# Start php-fpm
php-fpm -F &

wait
```

Note

- Git リポジトリにコミットする前に、startup.shファイルを実行可能ファイルとして保存してください。を使用してchmod +x startup.sh、 startup.sh ファイルに実行アクセス許可を設定します。
- startup.sh ファイルを実行可能ファイルとして保存しない場合は、apprunner.yamlファイルにbuildコマンドchmod +x startup.shとして と入力します。

Example apprunner.yaml

```
version: 1.0
```

```
runtime: php81
build:
  commands:
    build:
      - echo example build command for PHP
run:
  command: ./startup.sh
  network:
    port: 8080
    env: APP_PORT
```

Example index.php

```
<html>
<head> <title>First PHP App</title> </head>
<body>
<?php
    print("Hello World!");
    print("<br>");
?>
</body>
</html>
```

NGINX を使用して で PHP プラットフォームを実行する supervisord

Example ファイル構造

> **Note**
>
> - `supervisord.conf` ファイルはリポジトリ内の任意の場所に保存できます。`start` コマンドが`supervisord.conf`ファイルの保存先を指していることを確認します。
> - は、 `root` ディレクトリの `public`フォルダにインストール`index.php`する必要があります。

```
/
## public/
#  ## index.php
## apprunner.yaml
## supervisord.conf
```

Example supervisord.conf

```
[supervisord]
nodaemon=true

[program:nginx]
command=nginx -g "daemon off;"
autostart=true
autorestart=true
stdout_logfile=/dev/stdout
stdout_logfile_maxbytes=0
stderr_logfile=/dev/stderr
stderr_logfile_maxbytes=0

[program:php-fpm]
command=php-fpm -F
autostart=true
autorestart=true
stdout_logfile=/dev/stdout
stdout_logfile_maxbytes=0
stderr_logfile=/dev/stderr
stderr_logfile_maxbytes=0
```

Example apprunner.yaml

```
version: 1.0
runtime: php81
build:
  commands:
    build:
      - PYTHON=python2 amazon-linux-extras install epel
      - yum -y install supervisor
run:
  command: supervisord
  network:
    port: 8080
    env: APP_PORT
```

Example index.php

```
<html>
<head> <title>First PHP App</title> </head>
<body>
```

```
<?php
    print("Hello World!");
    print("<br>");
?>
</body>
</html>
```

NGINX を使用して で PHP プラットフォームを実行する startup script

Example ファイル構造

> **Note**
>
> - `startup.sh` ファイルはリポジトリ内の任意の場所に保存できます。`start` コマンドが`startup.sh`ファイルの保存先を指していることを確認します。
> - は、 `root` ディレクトリの `public`フォルダにインストール`index.php`する必要があります。

```
/
## public/
#  ## index.php
## apprunner.yaml
## startup.sh
```

Example startup.sh

```
#!/bin/bash

set -o monitor

trap exit SIGCHLD

# Start nginx
nginx -g 'daemon off;' &

# Start php-fpm
php-fpm -F &

wait
```

> **Note**
>
> - Git リポジトリにコミットする前に、`startup.sh`ファイルを実行可能ファイルとして保存してください。を使用して`chmod +x startup.sh`、 `startup.sh` ファイルに実行アクセス許可を設定します。
> - `startup.sh` ファイルを実行可能ファイルとして保存しない場合は、`apprunner.yaml`ファイルに`build`コマンド`chmod +x startup.sh`として と入力します。

Example apprunner.yaml

```
version: 1.0
runtime: php81
build:
  commands:
    build:
      - echo example build command for PHP
run:
  command: ./startup.sh
  network:
    port: 8080
    env: APP_PORT
```

Example index.php

```
<html>
<head> <title>First PHP App</title> </head>
<body>
<?php
    print("Hello World!");
    print("<br>");
?>
</body>
</html>
```

PHP ランタイムリリース情報

このトピックでは、App Runner がサポートする PHP ランタイムバージョンの詳細を一覧表示します。

サポートされているランタイムバージョン — 元の App Runner ビルド

ランタイム名	マイナーバージョン	含まれるパッケージ
PHP 8.1 (php81)	8.1.32	
	8.1.31	
	8.1.29	
	8.1.28	
	8.1.27	
	8.1.26	
	8.1.24	
	8.1.22	
	8.1.21	
	8.1.20	
	8.1.19	
	8.1.17	
	8.1.16	
	8.1.14	
	8.1.13	
	8.1.12	
	8.1.10	

> **Note**
>
> App Runner は、最近リリースされた特定の主要なランタイムに対して、改訂されたビルドプロセスを提供します。このため、このドキュメントの特定のセクションには、改訂された App Runner ビルドと元の App Runner ビルドへの参照が表示されます。詳細については、「マネージドランタイムバージョンと App Runner ビルド」を参照してください。

Ruby プラットフォームを使用する

AWS App Runner Ruby プラットフォームはマネージドランタイムを提供します。各ランタイムにより、Ruby バージョンに基づいてウェブアプリケーションを使用してコンテナを簡単に構築および実行できます。Ruby ランタイムを使用すると、App Runner はマネージド Ruby ランタイムイメージから開始します。このイメージは Amazon Linux Docker イメージに基づいており、Ruby のバージョンといくつかのツールのランタイムパッケージが含まれています。App Runner は、このマネージドランタイムイメージをベースイメージとして使用し、アプリケーションコードを追加して Docker イメージを構築します。次に、このイメージをデプロイして、コンテナでウェブサービスを実行します。

App Runner コンソールまたは CreateService API オペレーションを使用してサービスを作成するときに、App Runner サービスのランタイムを指定します。ソースコードの一部としてランタイムを指定することもできます。コードリポジトリに含める App Runner 設定ファイルで `runtime`キーワードを使用します。マネージドランタイムの命名規則は *`<language-name><major-version>`* です。

有効な Ruby ランタイム名とバージョンについては、「」を参照してくださいthe section called “リリース情報”。

App Runner は、デプロイまたはサービスの更新のたびに、サービスのランタイムを最新バージョンに更新します。アプリケーションで特定のバージョンのマネージドランタイムが必要な場合は、App Runner 設定ファイルの `runtime-version`キーワードを使用して指定できます。メジャーバージョンやマイナーバージョンなど、任意のレベルのバージョンにロックできます。App Runner は、サービスのランタイムに対してのみ低レベルの更新を行います。

Ruby ランタイムのバージョン構文: *`major`*`[.`*`minor`*`[.`*`patch`*`]]`

例: `3.1.2`

次の例は、バージョンロックを示しています。

- `3.1` – メジャーバージョンとマイナーバージョンをロックします。App Runner はパッチバージョンのみを更新します。
- `3.1.2` – 特定のパッチバージョンにロックします。App Runner はランタイムバージョンを更新しません。

トピック

- Ruby ランタイム設定
- Ruby ランタイムの例
- Ruby ランタイムリリース情報

Ruby ランタイム設定

マネージドランタイムを選択するときは、少なくとも コマンドを構築して実行するように設定する必要があります。App Runner サービスを作成または更新するときに設定します。これは、次のいずれかの方法を使用して実行できます。

- App Runner コンソールの使用 – 作成プロセスまたは設定タブのビルドの設定セクションでコマンドを指定します。
- App Runner API の使用 – CreateService または UpdateService API オペレーションを呼び出します。CodeConfigurationValues データ型の `BuildCommand`および `StartCommand`メンバーを使用してコマンドを指定します。
- 設定ファイルの使用 – 最大 3 つのビルドフェーズで 1 つ以上のビルドコマンドと、アプリケーションを起動する 1 つの実行コマンドを指定します。追加のオプションの設定があります。

設定ファイルの提供はオプションです。コンソールまたは API を使用して App Runner サービスを作成する場合、App Runner が作成時に設定を直接取得するか、設定ファイルから取得するかを指定します。

Ruby ランタイムの例

次の例は、Ruby サービスを構築および実行するための App Runner 設定ファイルを示しています。

最小 Ruby 設定ファイル

この例では、Ruby マネージドランタイムで使用できる最小限の設定ファイルを示しています。App Runner が最小限の設定ファイルで行う前提条件については、「」を参照してくださいthe section called “設定ファイルの例”。

Example apprunner.yaml

```
version: 1.0
runtime: ruby31
build:
  commands:
    build:
      - bundle install
run:
  command: bundle exec rackup --host 0.0.0.0 -p 8080
```

拡張 Ruby 設定ファイル

この例では、Ruby マネージドランタイムですべての設定キーを使用する方法を示します。

> **Note**
>
> これらの例で使用されるランタイムバージョンは *3.1.2* です。使用するバージョンに置き換えることができます。サポートされている最新の Ruby ランタイムバージョンについては、「」を参照してくださいthe section called “リリース情報”。

Example apprunner.yaml

```
version: 1.0
runtime: ruby31
build:
  commands:
     pre-build:
      - scripts/prebuild.sh
    build:
      - bundle install
    post-build:
      - scripts/postbuild.sh
  env:
```

```
    - name: MY_VAR_EXAMPLE
      value: "example"
run:
  runtime-version: 3.1.2
  command: bundle exec rackup --host 0.0.0.0 -p 4567
  network:
    port: 4567
    env: APP_PORT
  env:
    - name: MY_VAR_EXAMPLE
      value: "example"
```

Ruby アプリケーションソースを完了する

これらの例は、Ruby ランタイムサービスにデプロイできる完全な Ruby アプリケーションのソースコードを示しています。

Example server.rb

```
# server.rb
require 'sinatra'

get '/' do
  'Hello World!'
end
```

Example config.ru

```
# config.ru

require './server'

run Sinatra::Application
```

Example Gemfile

```
# Gemfile
source 'https://rubygems.org (https://rubygems.org/)'

gem 'sinatra'
gem 'puma'
```

Example apprunner.yaml

```
version: 1.0
runtime: ruby31
build:
  commands:
    build:
      - bundle install
run:
  command: bundle exec rackup --host 0.0.0.0 -p 4567
  network:
    port: 4567
    env: APP_PORT
```

Ruby ランタイムリリース情報

このトピックでは、App Runner がサポートする Ruby ランタイムバージョンの詳細を一覧表示します。

サポートされているランタイムバージョン — 元の App Runner ビルド

ランタイム名	マイナーバージョン	含まれるパッケージ
Ruby 3.1 (ruby31)	3.1.7	SQLite 3.50.0
	3.1.6	SQLite 3.49.1
	3.1.4	SQLite 3.46.0
	3.1.3	SQLite 3.41.0
	3.1.2	SQLite 3.39.4

> **Note**
>
> App Runner は、最近リリースされた特定のメジャーランタイムのビルドプロセスを改訂しました。このため、このドキュメントの特定のセクションには、改訂された App Runner ビルドと元の App Runner ビルドへの参照が表示されます。詳細については、「マネージドランタイムバージョンと App Runner ビルド」を参照してください。

Go プラットフォームを使用する

AWS App Runner Go プラットフォームはマネージドランタイムを提供します。各ランタイムにより、Go バージョンに基づいてウェブアプリケーションを使用してコンテナを簡単に構築および実行できます。Go ランタイムを使用すると、App Runner はマネージド Go ランタイムイメージから開始します。このイメージは Amazon Linux Docker イメージに基づいており、Go のバージョンといくつかのツールのランタイムパッケージが含まれています。App Runner は、このマネージドランタイムイメージをベースイメージとして使用し、アプリケーションコードを追加して Docker イメージを構築します。次に、このイメージをデプロイして、コンテナでウェブサービスを実行します。

App Runner コンソールまたは CreateService API オペレーションを使用してサービスを作成するときに、App Runner サービスのランタイムを指定します。ソースコードの一部としてランタイムを指定することもできます。コードリポジトリに含める App Runner 設定ファイルで `runtime`キーワードを使用します。マネージドランタイムの命名規則は *`<language-name><major-version>`* です。

有効な Go ランタイム名とバージョンについては、「」を参照してくださいthe section called “リリース情報”。

App Runner は、デプロイまたはサービスの更新のたびに、サービスのランタイムを最新バージョンに更新します。アプリケーションで特定のバージョンのマネージドランタイムが必要な場合は、App Runner 設定ファイルの `runtime-version`キーワードを使用して指定できます。メジャーバージョンやマイナーバージョンなど、任意のレベルのバージョンにロックできます。App Runner は、サービスのランタイムに対してのみ低レベルの更新を行います。

Go ランタイムのバージョン構文: *`major`*`[.`*`minor`*`[.`*`patch`*`]]`

例: `1.18.7`

次の例は、バージョンロックを示しています。

- `1.18` – メジャーバージョンとマイナーバージョンをロックします。App Runner はパッチバージョンのみを更新します。
- `1.18.7` – 特定のパッチバージョンにロックします。App Runner はランタイムバージョンを更新しません。

トピック

- Go ランタイム設定
- Go ランタイムの例

- Go ランタイムリリース情報

Go ランタイム設定

マネージドランタイムを選択するときは、少なくとも コマンドを構築して実行するように設定する必要があります。App Runner サービスを作成または更新するときに設定します。これは、次のいずれかの方法を使用して実行できます。

- App Runner コンソールの使用 – 作成プロセスまたは設定タブのビルドの設定セクションでコマンドを指定します。
- App Runner API の使用 – CreateService または UpdateService API オペレーションを呼び出します。CodeConfigurationValues データ型の `BuildCommand`および `StartCommand`メンバーを使用してコマンドを指定します。
- 設定ファイルの使用 – 最大 3 つのビルドフェーズで 1 つ以上のビルドコマンドと、アプリケーションを起動する 1 つの実行コマンドを指定します。追加のオプションの設定があります。

設定ファイルの提供はオプションです。コンソールまたは API を使用して App Runner サービスを作成する場合、App Runner が作成時に設定を直接取得するか、設定ファイルから取得するかを指定します。

Go ランタイムの例

次の例は、Go サービスを構築および実行するための App Runner 設定ファイルを示しています。

最小 Go 設定ファイル

この例は、Go マネージドランタイムで使用できる最小限の設定ファイルを示しています。App Runner が最小限の設定ファイルで行う前提条件については、「」を参照してくださいthe section called “設定ファイルの例”。

Example apprunner.yaml

```
version: 1.0
runtime: go1
build:
  commands:
    build:
      - go build main.go
run:
```

```
  command: ./main
```

拡張 Go 設定ファイル

この例では、Go マネージドランタイムですべての設定キーを使用する方法を示します。

> **Note**
>
> これらの例で使用されるランタイムバージョンは *1.18.7* です。使用するバージョンに置き換えることができます。サポートされている最新の Go ランタイムバージョンについては、「」を参照してくださいthe section called “リリース情報”。

Example apprunner.yaml

```
version: 1.0
runtime: go1
build:
  commands:
     pre-build:
      - scripts/prebuild.sh
    build:
      - go build main.go
    post-build:
      - scripts/postbuild.sh
  env:
    - name: MY_VAR_EXAMPLE
      value: "example"
run:
  runtime-version: 1.18.7
  command: ./main
  network:
    port: 3000
    env: APP_PORT
  env:
    - name: MY_VAR_EXAMPLE
      value: "example"
```

Go アプリケーションソースを完了する

これらの例は、Go ランタイムサービスにデプロイできる完全な Go アプリケーションのソースコードを示しています。

Example main.go

```
package main
import (
    "fmt"
    "net/http"
)

func main() {
    http.HandleFunc("/", func(w http.ResponseWriter, r *http.Request) {
        fmt.Fprint(w, "<h1>Welcome to App Runner</h1>")
    })
    fmt.Println("Starting the server on :3000...")
    http.ListenAndServe(":3000", nil)
}
```

Example apprunner.yaml

```
version: 1.0
runtime: go1
build:
  commands:
    build:
      - go build main.go
run:
  command: ./main
  network:
    port: 3000
    env: APP_PORT
```

Go ランタイムリリース情報

このトピックでは、App Runner がサポートする Go ランタイムバージョンの詳細を一覧表示します。

サポートされているランタイムバージョン — 元の App Runner ビルド

ランタイム名	マイナーバージョン	含まれるパッケージ
Go 1 (go1)	1.18.10	
	1.18.9	

ランタイム名	マイナーバージョン	含まれるパッケージ
	1.18.8	
	1.18.7	

> **Note**
>
> App Runner は、最近リリースされた特定のメジャーランタイムのビルドプロセスを改訂しました。このため、このドキュメントの特定のセクションには、改訂された App Runner ビルドと元の App Runner ビルドへの参照が表示されます。詳細については、「マネージドランタイムバージョンと App Runner ビルド」を参照してください。

App Runner のアプリケーションコードの開発

この章では、デプロイ先のアプリケーションコードを開発または移行する際に考慮すべきランタイム情報と開発ガイドラインについて説明します AWS App Runner。

ランタイム情報

コンテナイメージを提供するか、App Runner が構築するかにかかわらず、App Runner はコンテナインスタンスでアプリケーションコードを実行します。コンテナインスタンスのランタイム環境の主な側面を以下に示します。

- フレームワークのサポート – App Runner は、ウェブアプリケーションを実装するすべてのイメージをサポートします。選択したプログラミング言語や、使用するウェブアプリケーションサーバーまたはフレームワークには関係ありません。便宜上、さまざまなプログラミングプラットフォーム用のプラットフォーム固有のマネージドランタイムを提供し、アプリケーションビルドプロセスと抽象イメージの作成を合理化します。
- ウェブリクエスト – App Runner は、コンテナインスタンスに HTTP 1.0 および HTTP 1.1 のサポートを提供します。サービスの設定の詳細については、「」を参照してくださいthe section called “設定”。HTTPS セキュアトラフィックの処理を実装する必要はありません。App Runner は、すべての受信 HTTP リクエストを対応する HTTPS エンドポイントにリダイレクトします。HTTP ウェブリクエストのリダイレクトを有効にする設定は必要ありません。App Runner は、アプリケーションコンテナインスタンスにリクエストを渡す前に TLS を終了します。

> **Note**
>
> - HTTP リクエストには合計 120 秒のリクエストタイムアウト制限があります。120 秒には、本文を含むリクエストの読み取りと HTTP レスポンスの書き込み完了にアプリケーションがかかる時間が含まれます。
> - リクエストの読み取りとレスポンスのタイムアウトの制限は、使用するアプリケーションによって異なります。これらのアプリケーションには、Python 用の HTTP サーバー、Gunicorn など、独自の内部タイムアウトがあり、デフォルトのタイムアウト制限は 30 秒です。このような場合、アプリケーションのタイムアウト制限は App Runner の 120 秒のタイムアウト制限よりも優先されます。
> - App Runner はフルマネージドサービスであるため、TLS 暗号スイートやその他のパラメータを設定する必要はありません。TLS 終了は によって管理されます。

- ステートレスアプリ – 現在、App Runner はステートフルアプリをサポートしていません。したがって、App Runner は、単一の受信ウェブリクエストを処理する期間を超えて状態が永続化することを保証しません。
- ストレージ – App Runner は、受信トラフィック量に応じて App Runner アプリケーションのインスタンスを自動的にスケールアップまたはスケールダウンします。App Runner アプリケーションの Auto Scaling オプションを設定できます。ウェブリクエストを処理する現在アクティブなインスタンスの数は受信トラフィック量に基づいているため、App Runner は 1 つのリクエストの処理を超えてファイルが保持できることを保証できません。したがって、App Runner はコンテナインスタンスにファイルシステムをエフェメラルストレージとして実装します。そのため、ファイルは一時的なものです。例えば、App Runner サービスを一時停止して再開しても、ファイルは保持されません。

  App Runner は 3 GB のエフェメラルストレージを提供し、インスタンスのプル、圧縮、および非圧縮コンテナイメージに 3 GB のエフェメラルストレージの一部を使用します。残りのエフェメラルストレージは App Runner サービスで使用できます。ただし、ステートレスであるため、これは永続的ストレージではありません。

  > **Note**
  >
  > ストレージファイルがリクエスト間で保持されるシナリオが発生する場合があります。例えば、次のリクエストが同じインスタンスに送信された場合、ストレージファイルは保持されます。リクエスト間でのストレージファイルの永続化は、特定の状況で役立ちます。例えば、リクエストを処理するときに、今後のリクエストで必要になる可能性がある場合は、アプリケーションがダウンロードしたファイルをキャッシュできます。これにより、将来のリクエスト処理が高速化される可能性がありますが、速度の向上は保証できません。コードでは、前のリクエストでダウンロードされたファイルがまだ存在すると想定しないでください。
  >
  > 高スループット、低レイテンシーのインメモリデータストアを使用したキャッシュが保証されるようにするには、Amazon ElastiCache などのサービスを使用します。

- 環境変数 – デフォルトでは、App Runner はPORT環境変数をコンテナインスタンスで使用できるようにします。ポート情報を使用して変数値を設定し、カスタム環境変数と値を追加できます。AWS Secrets Manager または AWS Systems Manager Parameter Store に保存されている機密データを環境変数として参照することもできます。環境変数の作成の詳細については、「」を参照してくださいリファレンス環境変数。
- インスタンスロール – アプリケーションコードが AWS サービス APIs またはいずれかの AWS SDKs を使用して任意のサービスを呼び出す場合は、 AWS Identity and Access Management

(IAM) を使用してインスタンスロールを作成します。次に、作成時に App Runner サービスにアタッチします。コードが必要とするすべての AWS サービスアクションのアクセス許可をインスタンスロールに含めます。詳細については、「the section called “インスタンスロール”」を参照してください。

コード開発ガイドライン

App Runner ウェブアプリケーションのコードを開発するときは、以下のガイドラインを考慮してください。

- コンテナイメージへのパッチ適用 – コンテナイメージを提供する場合、これらのイメージを定期的に更新してパッチを適用する責任があります。App Runner がインフラストラクチャを管理する間、提供されたコンテナイメージのセキュリティとup-to-dateステータスを確認する必要があります。詳細については、AWS App Runner ドキュメントを参照してください。
- ステートレスコードを設計する – App Runner サービスにデプロイするウェブアプリケーションをステートレスに設計します。コードでは、単一の受信ウェブリクエストを処理する期間を超えて状態が保持されないことを前提とする必要があります。
- 一時ファイルの削除 – ファイルを作成すると、ファイルはファイルシステムに保存され、サービスのストレージ割り当ての一部になります。out-of-storageエラーを避けるため、一時ファイルを長期間保持しないでください。ファイルキャッシュの決定を行うときは、ストレージサイズとリクエスト処理速度のバランスを取ります。
- インスタンスの起動 – App Runner はインスタンスの起動時間を 5 分提供します。インスタンスは、設定されたリッスンポートでリクエストをリッスンし、起動から 5 分以内に正常である必要があります。起動時に、App Runner インスタンスには vCPU 設定に基づいて仮想 CPU (vCPU) が割り当てられます。使用可能な vCPU 設定の詳細については、「」を参照してくださいthe section called “App Runner でサポートされている設定”。

  インスタンスが正常に起動すると、アイドル状態になり、リクエストを待機します。料金は、インスタンスの起動時間に基づいて支払います。最低料金は、インスタンスの起動ごとに 1 分です。料金については、「AWS App Runner の料金」を参照してください。

App Runner コンソールの使用

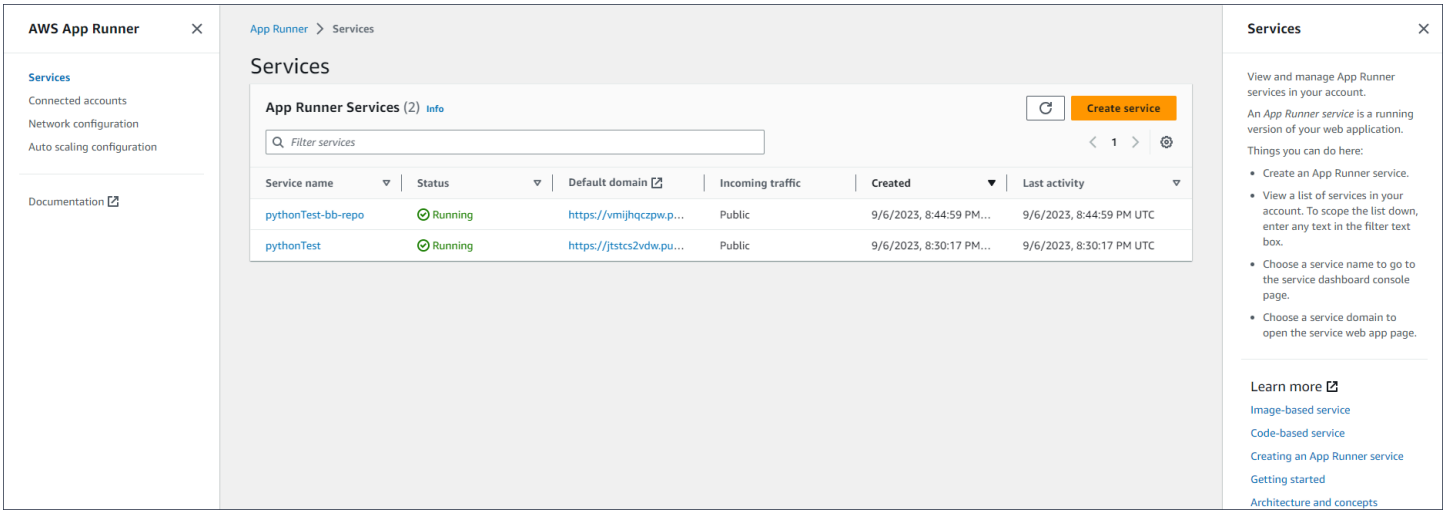
AWS App Runner コンソールを使用して、接続されたアカウントなどの App Runner サービスおよび関連リソースを作成、管理、モニタリングします。既存のサービスの表示、新しいサービスの作成、サービスの設定を行うことができます。App Runner サービスのステータスの表示、ログの表示、アクティビティのモニタリング、メトリクスの追跡を行うことができます。サービスのウェブサイトまたはソースリポジトリに移動することもできます。

以下のセクションでは、コンソールのレイアウトと機能について説明し、関連情報を示します。

コンソール全体のレイアウト

App Runner コンソールには 3 つの領域があります。左から右へ：

- ナビゲーションペイン – 折りたたんだり展開したりできるサイドペイン。これを使用して、使用する最上位コンソールページを選択します。
- コンテンツペイン – コンソールページのメイン部分。これを使用して情報を表示し、タスクを実行します。
- ヘルプペイン – 詳細については、サイドペインを参照してください。これを展開すると、現在使用しているページに関するヘルプが表示されます。または、コンソールページで任意の情報リンクを選択して、コンテキストヘルプを取得します。



サービスページ

サービスページには、アカウントの App Runner サービスが一覧表示されます。フィルターテキストボックスを使用して、リストの範囲を絞り込むことができます。

サービスページに移動するには

1. App Runner コンソールを開き、リージョンリストで を選択します AWS リージョン。
2. ナビゲーションペインで [Services (サービス)] を選択します。

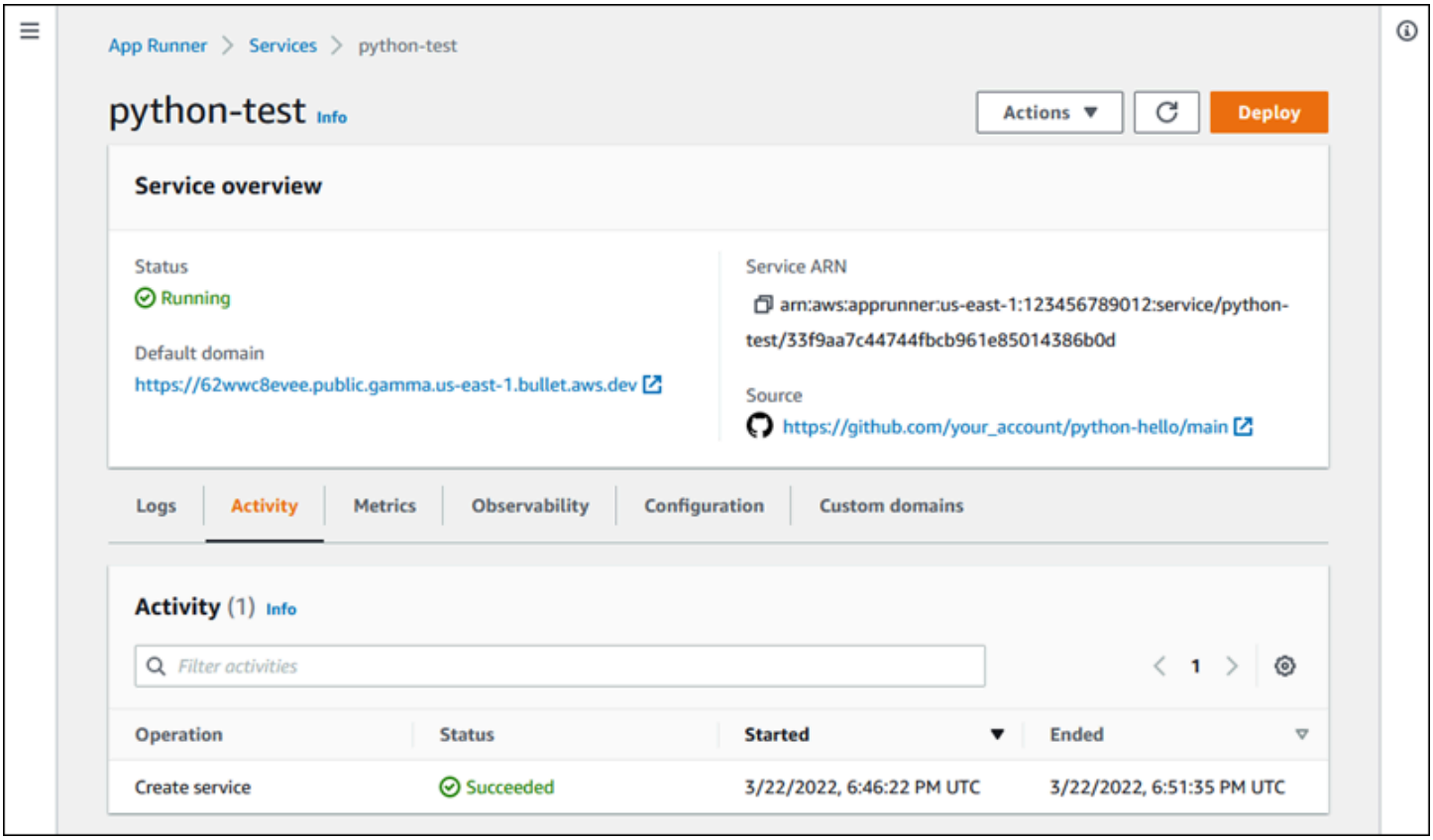
ここでできること：

- App Runner サービスを作成します。詳細については、「the section called “作成”」を参照してください。
- サービス名を選択して、サービスダッシュボードコンソールページに移動します。
- サービスドメインを選択して、サービスウェブアプリページを開きます。

サービスダッシュボードページ

App Runner サービスに関する情報を表示し、サービスダッシュボードページから管理できます。ページの上部にサービス名が表示されます。

サービスダッシュボードにアクセスするには、サービスページに移動し (前のセクションを参照) 、App Runner サービスを選択します。



サービスの概要セクションには、App Runner サービスとアプリケーションに関する基本的な詳細が表示されます。ここでできること：

- ステータス、ヘルス、ARN などのサービスの詳細を表示します。
- デフォルトドメインに移動します。デフォルトドメインは、サービスで実行されているウェブアプリケーション用に App Runner が提供するドメインです。これは App Runner が所有するドメインのサブ`awsapprunner.com`ドメインです。
- サービスにデプロイされたソースリポジトリに移動します。
- サービスへのソースリポジトリのデプロイを開始します。
- サービスを一時停止、再開、削除します。

サービスの概要の下のタブは、サービス管理とオブザーバビリティ用です。

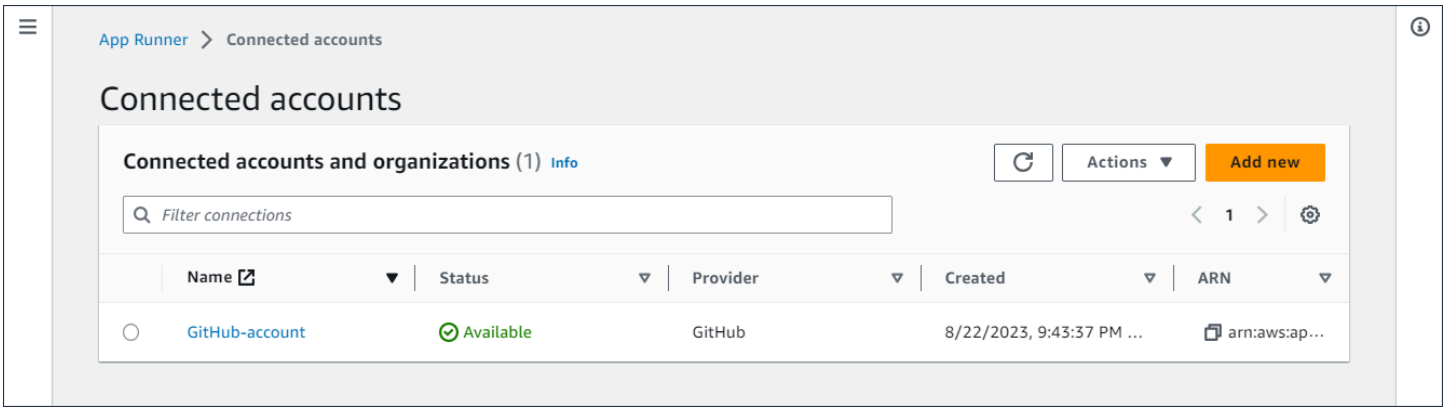
接続されたアカウントページ

接続されたアカウントページには、アカウントのソースコードリポジトリプロバイダーへの App Runner 接続が一覧表示されます。フィルターテキストボックスを使用して、リストの範囲を絞り込

むことができます。接続されたアカウントの詳細については、「」を参照してくださいthe section called “Connections”。

接続されたアカウントページに移動するには

1. App Runner コンソールを開き、リージョンリストで を選択します AWS リージョン。
2. ナビゲーションペインで、接続されたアカウントを選択します。



ここでできること：

- アカウントのリポジトリプロバイダー接続のリストを表示します。リストの範囲を絞り込むには、フィルターテキストボックスに任意のテキストを入力します。
- 接続名を選択して、関連するプロバイダーアカウントまたは組織に移動します。
- 接続を選択して、（サービスの作成の一環として）確立した接続のハンドシェイクを完了するか、接続を削除します。

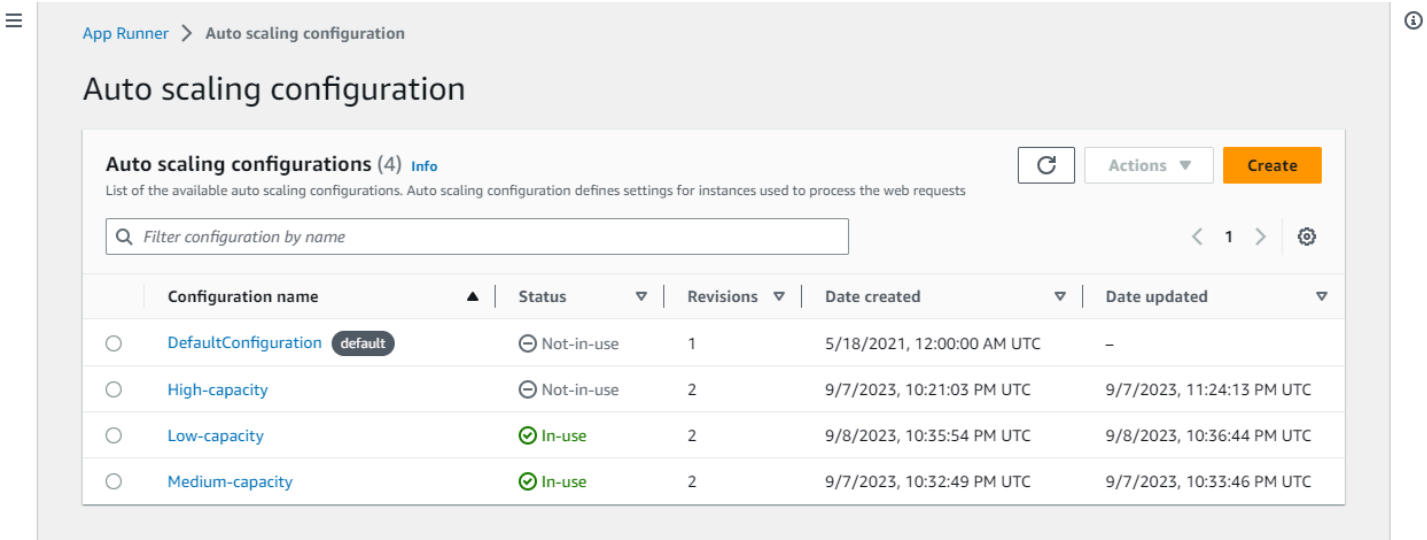
Auto Scaling 設定ページ

Auto Scaling 設定ページには、アカウントで設定した Auto Scaling 設定が一覧表示されます。自動スケーリングの動作を調整し、後で 1 つ以上の App Runner サービスに割り当てることができるさまざまな設定に保存するように、いくつかのパラメータを設定できます。フィルターテキストボックスを使用して、リストの範囲を絞り込むことができます。自動スケーリング設定の詳細については、「」を参照してくださいサービスの自動スケーリングを管理する。

Auto Scaling 設定ページに移動するには

1. App Runner コンソールを開き、リージョンリストで を選択します AWS リージョン。

2. ナビゲーションペインで、Auto Scaling 設定を選択します。



ここでできること：

- アカウントの既存の Auto Scaling 設定のリストを表示します。
- 新しい自動スケーリング設定または既存の設定のリビジョンを作成します。
- 自動スケーリング設定を、作成する新しいサービスのデフォルトとして設定します。
- 設定を削除します。
- 設定の名前を選択して Auto Scaling リビジョンパネルに移動し、リビジョンを管理します。

App Runner サービスの管理

この章では、 AWS App Runner サービスを管理する方法について説明します。この章では、サービスの作成、設定、削除、新しいアプリケーションバージョンのサービスへのデプロイ、サービスの一時停止と再開によるウェブサービスの可用性の制御など、サービスのライフサイクルを管理する方法について説明します。また、接続や自動スケーリングなど、サービスの他の側面を管理する方法についても説明します。

トピック

- App Runner サービスの作成
- 失敗した App Runner サービスの再構築
- App Runner への新しいアプリケーションバージョンのデプロイ
- App Runner サービスの設定
- App Runner 接続の管理
- App Runner 自動スケーリングの管理
- App Runner サービスのカスタムドメイン名の管理
- App Runner サービスの一時停止と再開
- App Runner サービスの削除

App Runner サービスの作成

AWS App Runner は、コンテナイメージまたはソースコードリポジトリから、自動的にスケールする実行中のウェブサービスへの移行を自動化します。App Runner をソースイメージまたはコードにポイントし、少数の必要な設定のみを指定します。App Runner は、必要に応じてアプリケーションを構築し、コンピューティングリソースをプロビジョニングし、アプリケーションを実行してデプロイします。

サービスを作成すると、App Runner はサービスリソースを作成します。場合によっては、接続リソースを提供する必要があります。App Runner コンソールを使用する場合、コンソールは接続リソースを暗黙的に作成します。App Runner リソースタイプの詳細については、「」を参照してくださいthe section called “App Runner リソース”。これらのリソースタイプには、各 のアカウントに関連付けられたクォータがあります AWS リージョン。詳細については、「the section called “App Runner リソースクォータ”」を参照してください。

ソースタイプとプロバイダーに応じて、サービスを作成する手順に微妙な違いがあります。このトピックでは、状況に適したものに従うことができるように、これらのソースタイプを作成するさまざまな手順について説明します。コード例を使用して基本的な手順を開始するには、「」を参照してください入門。

前提条件

App Runner サービスを作成する前に、必ず次のアクションを実行してください。

- のセットアップ手順を完了します設定。
- アプリケーションソースの準備が整っていることを確認します。GitHub のコードリポジトリ、Bitbucket、または Amazon Elastic Container Registry (Amazon ECR) のコンテナイメージのいずれかを使用して、App Runner サービスを作成できます。

サービスを作成する

このセクションでは、ソースコードに基づく とコンテナイメージに基づく 2 つの App Runner サービスタイプの作成プロセスについて説明します。

> **Note**
>
> サービスのアウトバウンドトラフィック VPC コネクタを作成すると、次のサービス起動プロセスで 1 回限りのレイテンシーが発生します。この設定は、新しいサービスの作成時または作成後にサービスの更新で設定できます。詳細については、このガイド1 回限りのレイテンシーの「Networking with App Runner」の章の「」を参照してください。

コードリポジトリからサービスを作成する

以下のセクションでは、ソースが GitHub または Bitbucket のコードリポジトリである場合に App Runner サービスを作成する方法を示します。コードリポジトリを使用する場合、App Runner はプロバイダーの組織またはアカウントに接続する必要があります。したがって、この接続の確立を支援する必要があります。App Runner 接続の詳細については、「」を参照してくださいthe section called “Connections”。

サービスを作成すると、App Runner はアプリケーションコードと依存関係を含む Docker イメージを構築します。次に、このイメージのコンテナインスタンスを実行するサービスを起動します。

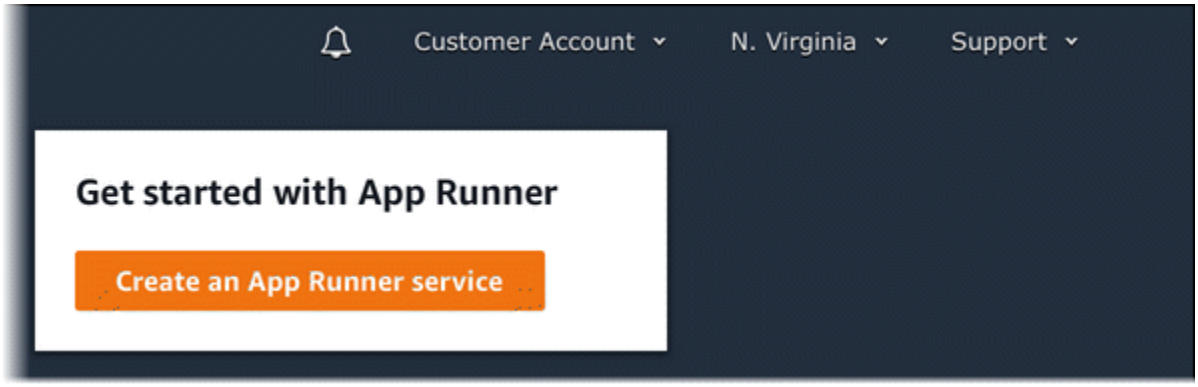
App Runner コンソールを使用してコードからサービスを作成する

コンソールを使用して App Runner サービスを作成するには

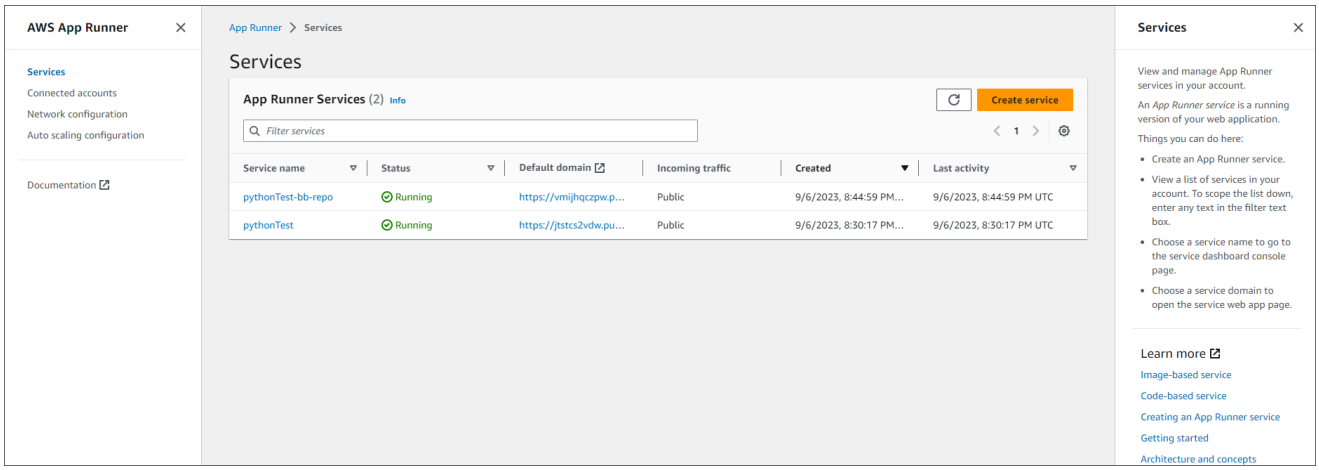
1. ソースコードを設定します。

   a. App Runner コンソールを開き、リージョンリストで を選択します AWS リージョン。

   b. AWS アカウント に App Runner サービスがまだない場合は、コンソールのホームページが表示されます。App Runner サービスの作成を選択します。



   に既存のサービス AWS アカウント がある場合、サービスのリストを含むサービスページが表示されます。[Create service (サービスの作成)] を選択します。



   c. 「ソースとデプロイ」ページの「ソース」セクションの「リポジトリタイプ」で、「ソースコードリポジトリ」を選択します。

   d. プロバイダータイプを選択します。GitHub または Bitbucket を選択します。

   e. 次に、以前に使用したプロバイダーのアカウントまたは組織を選択するか、新規追加を選択します。次に、コードリポジトリの認証情報を提供し、接続するアカウントまたは組織を選択するプロセスを実行します。

f. リポジトリ で、アプリケーションコードを含むリポジトリを選択します。

g. Branch で、デプロイするブランチを選択します。

h. Source ディレクトリには、アプリケーションコードと設定ファイルを保存するソースリポジトリに ディレクトリを入力します。

> **Note**
>
> ビルドコマンドとスタートコマンドは、指定したソースディレクトリから実行されます。App Runner はルートからの絶対パスとして処理します。ここで値を指定しない場合、ディレクトリはデフォルトでリポジトリルートになります。

2. デプロイを設定します。

   a. デプロイ設定セクションで、手動または自動を選択します。

      デプロイ方法の詳細については、「」を参照してくださいthe section called “デプロイ方法”。

   b. [次へ] を選択します。

Source and deployment Info

Choose the source for your App Runner service and the way it's deployed.

Source and deployment

Source

Repository type

- ○ Container registry
  Deploy your service using a container image stored in a container registry.
- ◉ Source code repository
  Deploy your service using the code hosted in a source repository.

Provider
Choose the provider where you host your code repository.

GitHub

Github Connection Info

App Runner deploys your source code by installing an app called "AWS Connector for GitHub" in your account. You can install this app in your main GitHub account or in a GitHub organization.

myGitHub | Add new

Repository

python-hello

Branch

main

Source directory
The build and start commands will execute in this directory. App Runner defaults to the root directory if you don't specify a directory here.

/

Leading and trailing slashes ("/") are not required. Valid examples: "apps/targetapp", "/apps/targetapp/", "/targetapp"

Deployment settings

Deployment trigger

- ○ Manual
  Start each deployment yourself using the App Runner console or AWS CLI.
- ◉ Automatic
  Every push to this branch that affects files in the specified **Source directory** deploys a new version of your service.

Cancel | Next

3. アプリケーションビルドを設定します。

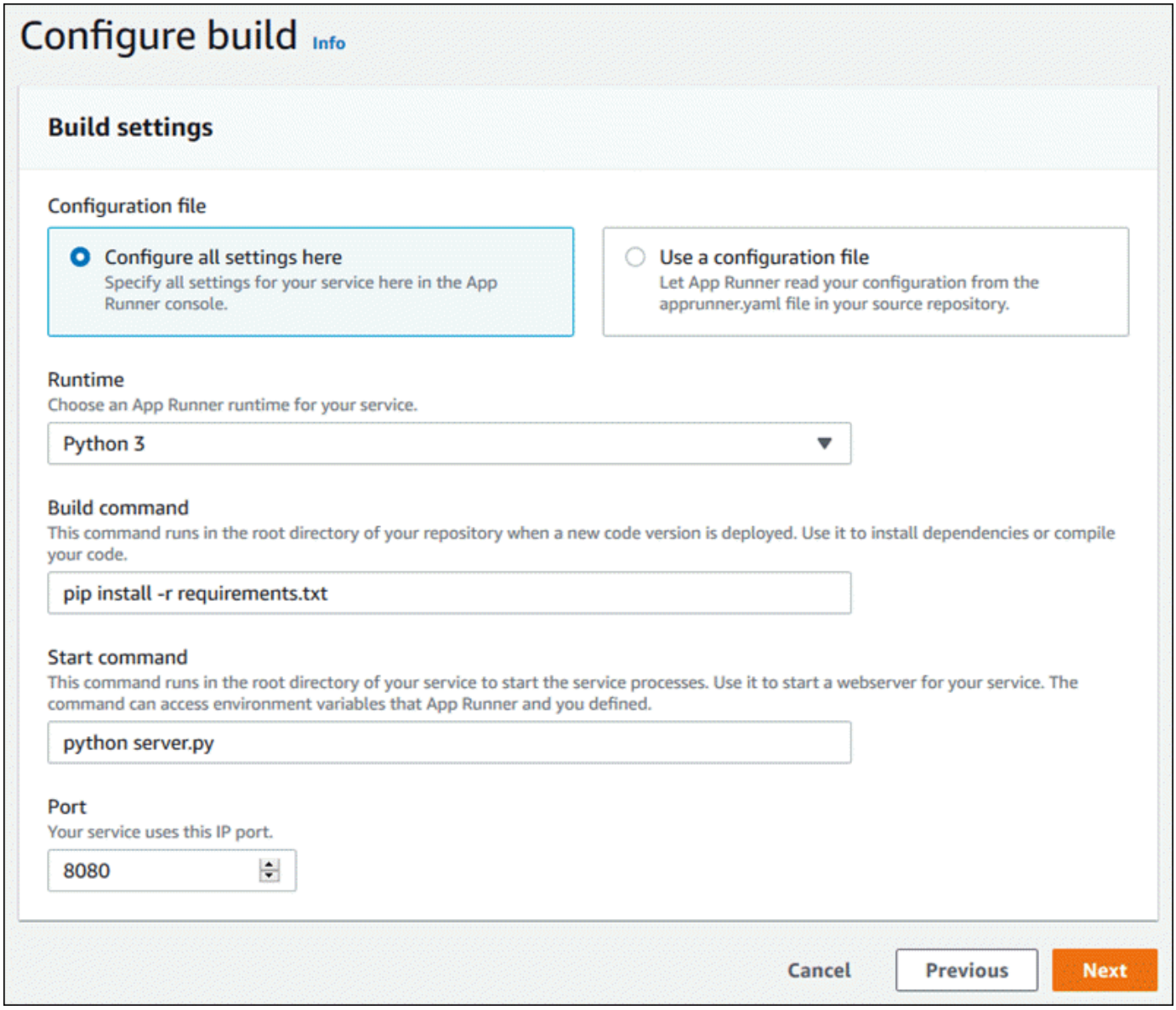
   a. 「ビルドの設定」ページの「設定ファイル」で、リポジトリに App Runner 設定ファイルが含まれていない場合はここですべての設定を設定する」を選択するか、含まれている場合は設定ファイルを使用するを選択します。

   > **Note**
   >
   > App Runner 設定ファイルは、アプリケーションソースの一部としてビルド設定を維持する方法です。指定すると、App Runner はファイルからいくつかの値を読み取り、コンソールで設定することはできません。

   b. 次のビルド設定を指定します。

      - ランタイム – アプリケーションの特定のマネージドランタイムを選択します。
      - ビルドコマンド – ソースコードからアプリケーションを構築するコマンドを入力します。これは、言語固有のツールでも、コードに付属のスクリプトでもかまいません。
      - Start command – ウェブサービスを開始するコマンドを入力します。
      - ポート – ウェブサービスがリッスンする IP ポートを入力します。

   c. [次へ] を選択します。



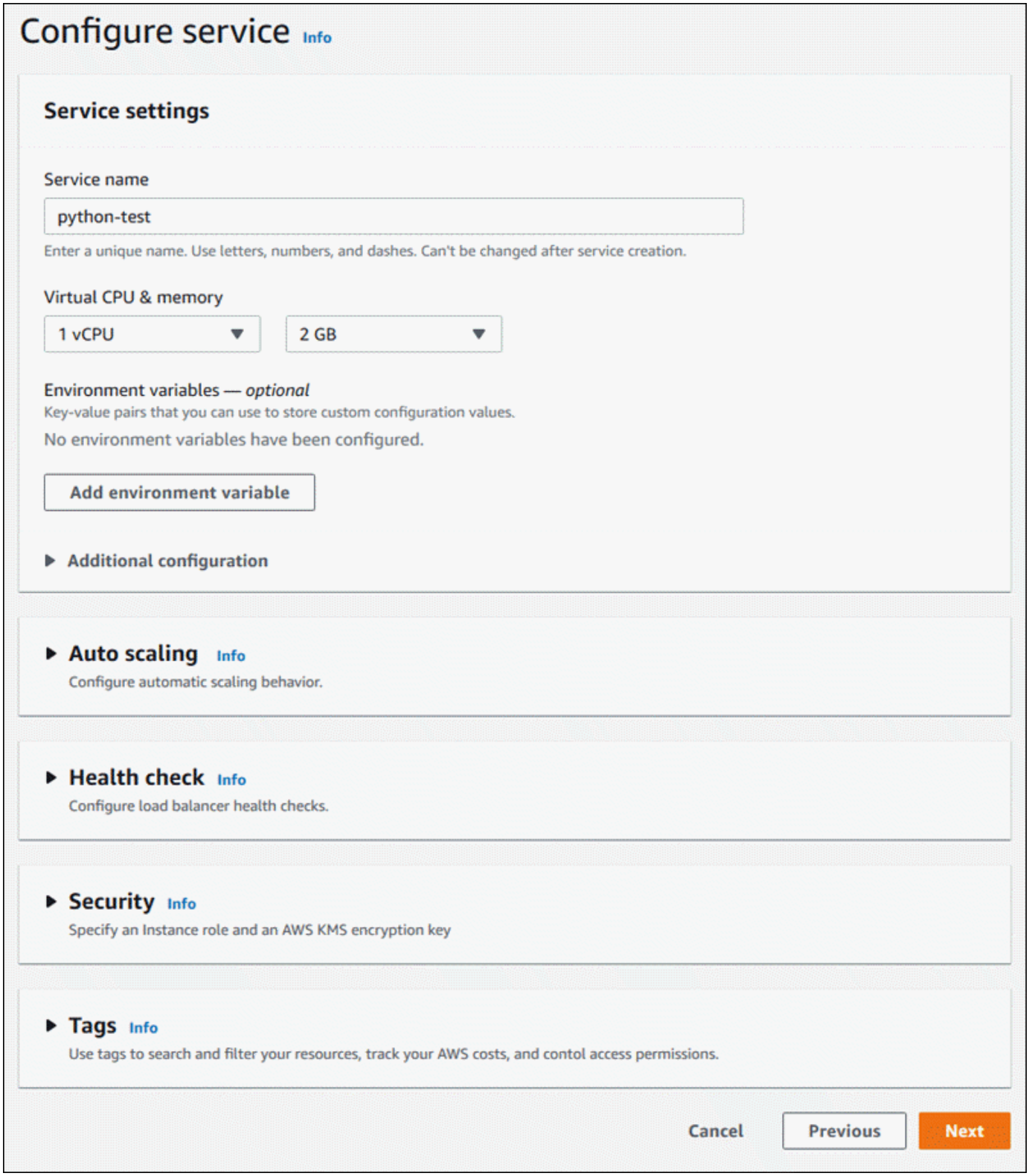
4. サービスを設定します。

   a. 「サービスの設定」ページの「サービス設定」セクションに、サービス名を入力します。

   > **Note**
   >
   > その他のサービス設定はすべてオプションであるか、コンソールが提供するデフォルトです。

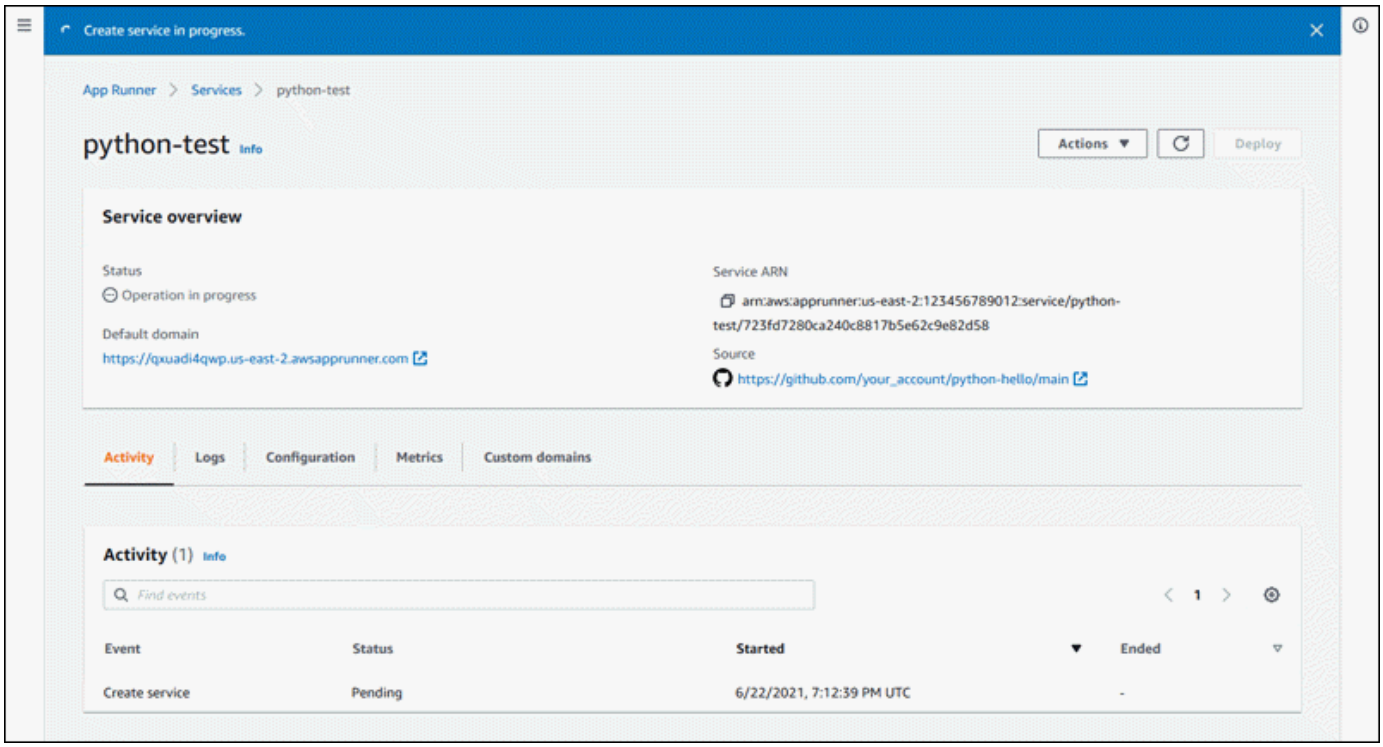
   b. 必要に応じて、アプリケーション要件を満たすように他の設定を変更または追加します。

c. [次へ] を選択します。


Configure service Info
Service settings
Service name
python-test
Enter a unique name. Use letters, numbers, and dashes. Can't be changed after service creation.
Virtual CPU & memory
1 vCPU
2 GB
Environment variables — optional
Key-value pairs that you can use to store custom configuration values.
No environment variables have been configured.
Add environment variable
Additional configuration
Auto scaling Info
Configure automatic scaling behavior.
Health check Info
Configure load balancer health checks.
Security Info
Specify an Instance role and an AWS KMS encryption key
Tags Info
Use tags to search and filter your resources, track your AWS costs, and contol access permissions.
Cancel
Previous
Next

5. 確認と作成ページで、入力したすべての詳細を確認し、作成とデプロイを選択します。

   結果: サービスが正常に作成されると、コンソールにサービスダッシュボードに新しいサービスの概要が表示されます。



6. サービスが実行されていることを確認します。

   a. サービスダッシュボードページで、サービスのステータスが実行中になるまで待ちます。

   b. デフォルトのドメイン値を選択します。これは、サービスのウェブサイトへの URL です。

   c. ウェブサイトを使用して、正しく実行されていることを確認します。

App Runner API または を使用してコードからサービスを作成する AWS CLI

App Runner API または を使用してサービスを作成するには AWS CLI、 `CreateService` API アクションを呼び出します。詳細と例については、「CreateService」を参照してください。ソースコードリポジトリ (GitHub または Bitbucket) の特定の組織またはアカウントを使用してサービスを作成するのが初めての場合は、まず CreateConnection を呼び出します。これにより、App Runner とリポジトリプロバイダーの組織またはアカウント間の接続が確立されます。App Runner 接続の詳細については、「」を参照してくださいthe section called “Connections”。

呼び出しが を示すサービスオブジェクトで成功したレスポンスを返すと`"Status": "CREATING"`、サービスの作成が開始されます。

呼び出しの例については、 AWS App Runner API リファレンスの「ソースコードリポジトリサービスの作成」を参照してください。

Amazon ECR イメージからサービスを作成する

以下のセクションでは、ソースが Amazon ECR に保存されているコンテナイメージである場合に App Runner サービスを作成する方法を示します。Amazon ECR は です AWS のサービス。したがって、Amazon ECR イメージに基づいてサービスを作成するには、必要な Amazon ECR アクションのアクセス許可を含むアクセスロールを App Runner に提供します。

> **Note**
>
> Amazon ECR Public に保存されているイメージは公開されています。したがって、イメージが Amazon ECR Public に保存されている場合、アクセスロールは必要ありません。

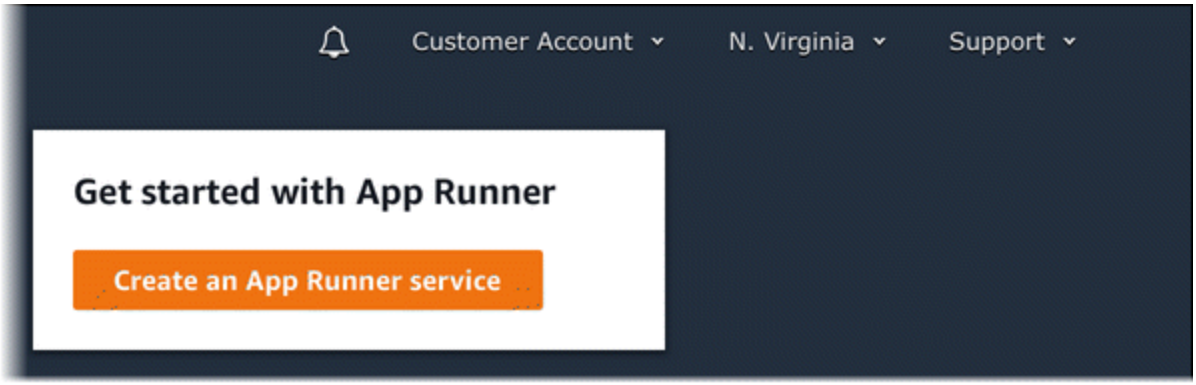
サービスが作成されると、App Runner は、指定したイメージのコンテナインスタンスを実行するサービスを起動します。この場合、ビルドフェーズはありません。

詳細については、「イメージベースのサービス」を参照してください。

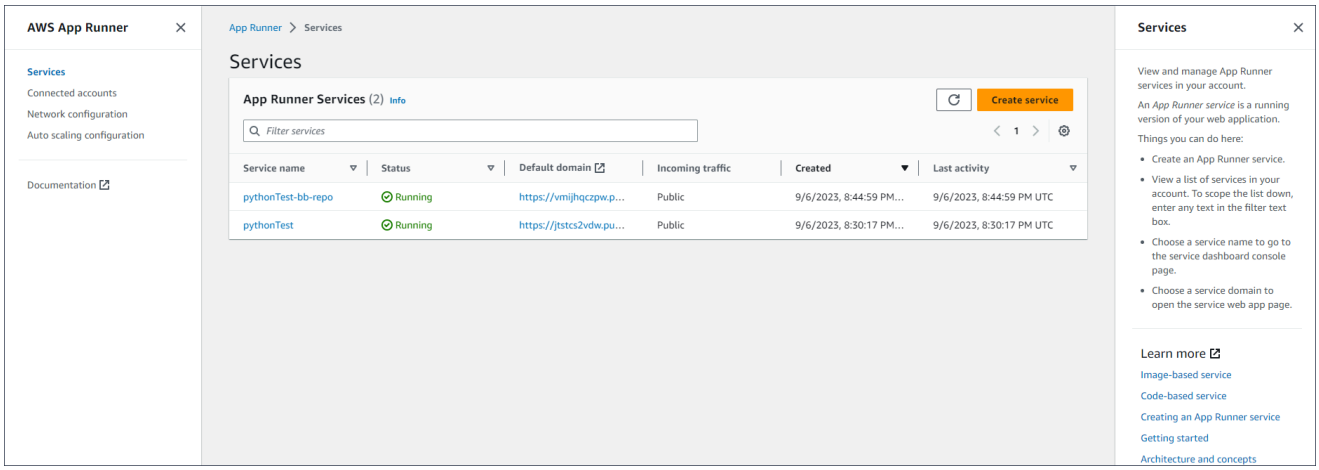
App Runner コンソールを使用したイメージからのサービスの作成

コンソールを使用して App Runner サービスを作成するには

1. ソースコードを設定します。
   a. App Runner コンソールを開き、リージョンリストで を選択します AWS リージョン。
   b. AWS アカウント に App Runner サービスがまだない場合は、コンソールのホームページが表示されます。App Runner サービスの作成を選択します。



に既存のサービス AWS アカウント がある場合、サービスのリストを含むサービスページが表示されます。[Create service (サービスの作成)] を選択します。



c. 「ソースとデプロイ」ページの「ソース」セクションの「リポジトリタイプ」で、「コンテナレジストリ」を選択します。

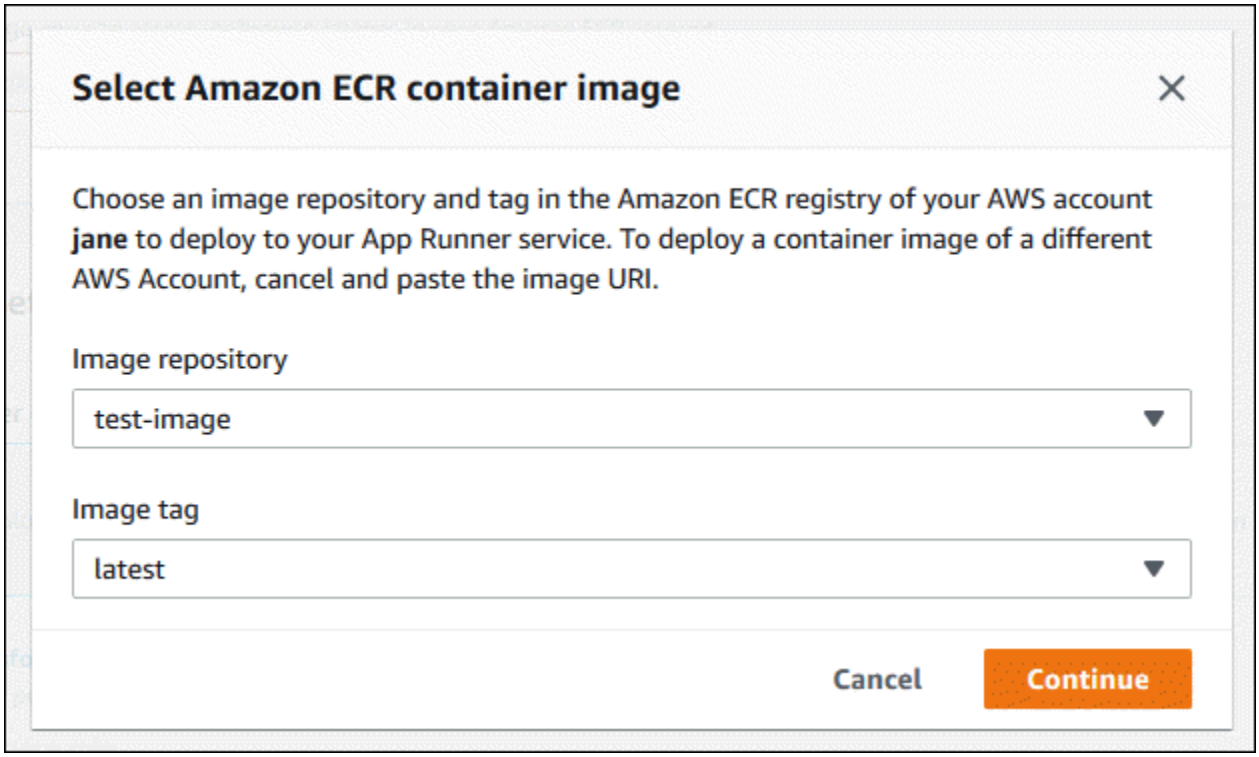
d. Provider で、イメージが保存されているプロバイダーを選択します。

- Amazon ECR – Amazon ECR に保存されているプライベートイメージ。
- Amazon ECR Public – Amazon ECR Public に保存されているパブリックに読み取り可能なイメージ。

e. コンテナイメージ URI で、参照 を選択します。

f. Amazon ECR コンテナイメージの選択ダイアログボックスの Image リポジトリで、イメージを含むリポジトリを選択します。

g. イメージタグで、デプロイする特定のイメージタグ (最新など) を選択し、続行を選択します。



2. デプロイを設定します。

   a. デプロイ設定セクションで、手動または自動を選択します。

   > **Note**
   >
   > App Runner は、Amazon ECR Public イメージ、およびサービスが存在するアカウントとは異なる AWS アカウントに属する Amazon ECR リポジトリ内のイメージの自動デプロイをサポートしていません。

   デプロイ方法の詳細については、「」を参照してくださいthe section called “デプロイ方法”。

   b. 〔Amazon ECR プロバイダー] ECR アクセスロールの場合は、アカウント内の既存のサービスロールを選択するか、新しいロールの作成を選択します。手動デプロイを使用している場合は、デプロイ時に IAM ユーザーロールを使用することもできます。

   c. [次へ] を選択します。

Source and deployment Info

Choose the source for your App Runner service and the way it's deployed.

Source

Repository type

- (●) Container registry
  Deploy your service from a container image stored in a container registry.
- ( ) Source code repository
  Deploy your service from code hosted in a source code repository.

Provider

- (●) Amazon ECR
- ( ) Amazon ECR Public

Container image URI

Enter a URI to an image you can access, or browse images in your Amazon ECR account.

123456789012.dkr.ecr.us-east-2.amazonaws.com/test-image:latest [Browse]

Deployment settings

Deployment trigger

- ( ) Manual
  Start each deployment yourself using the App Runner console or AWS CLI.
- (●) Automatic
  App Runner monitors your registry and deploys a new version of your service for each image push.

ECR access role Info

This role gives App Runner permission to access ECR. To create a custom role, go to the IAM console

- (●) Create new service role
- ( ) Use existing service role

Service role name

The name of an IAM role that App Runner creates in your account with an attached managed policy for ECR access.

AppRunnerECRAccessRole

[Cancel] [Next]

3. サービスを設定します。

   a. 「サービスの設定」ページの「サービス設定」セクションに、サービス名とサービスウェブサイトがリッスンする IP ポートを入力します。

   > **Note**
   >
   > その他のサービス設定はすべてオプションであるか、コンソールが提供するデフォルトです。

   b. (オプション) アプリケーションのニーズに応じて、他の設定を変更または追加します。

   c. [次へ] を選択します。

Configure service Info

Service settings

Service name

image-test

Enter a unique name. Use letters, numbers, and dashes. Can't be changed after service creation.

Virtual CPU & memory

1 vCPU | 2 GB

Environment variables — *optional*

Key-value pairs that you can use to store custom configuration values.

No environment variables have been configured.

Add environment variable

Port

Your service uses this IP port.

8080

▶ Additional configuration

▶ **Auto scaling** Info

Configure automatic scaling behavior.

▶ **Health check** Info

Configure load balancer health checks.

▶ **Security** Info

Specify an Instance role and an AWS KMS encryption key

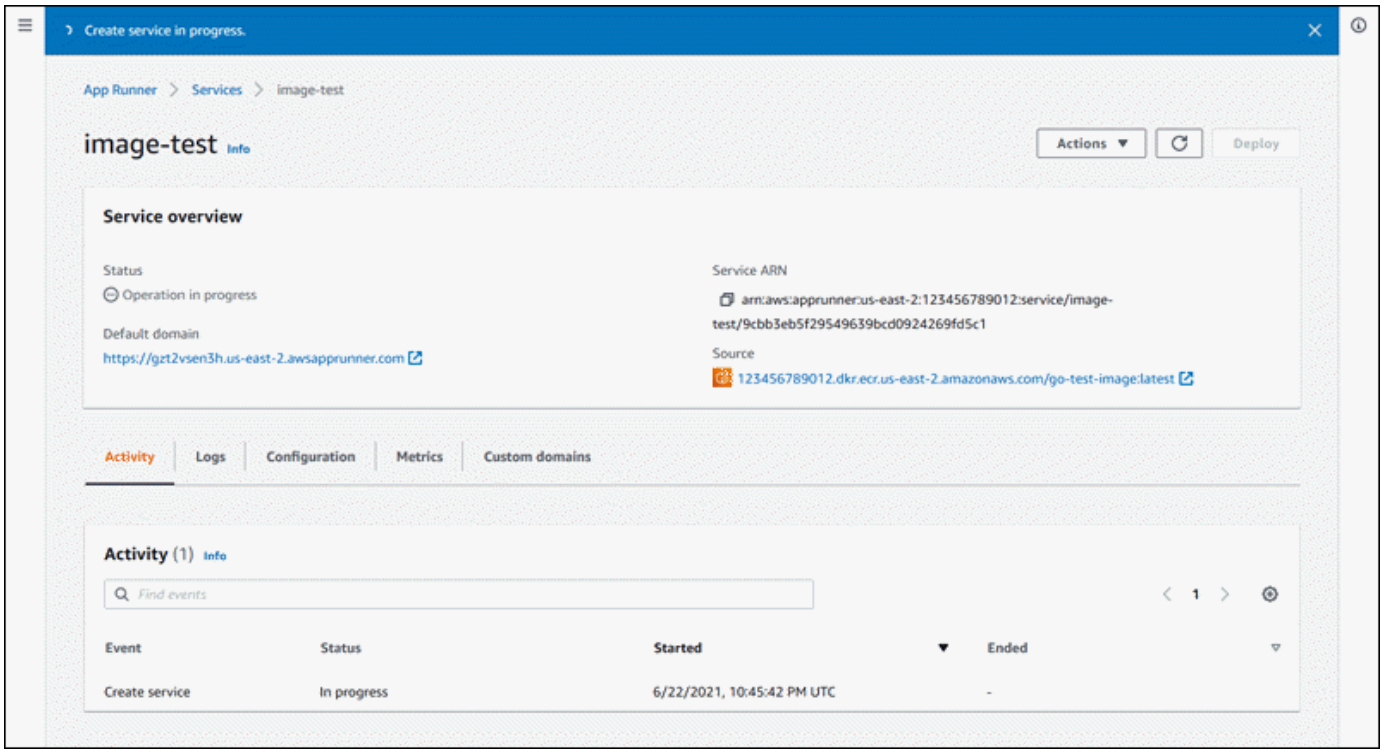
▶ **Tags** Info

Use tags to search and filter your resources, track your AWS costs, and contol access permissions.

Cancel | Previous | Next

4. 確認と作成ページで、入力したすべての詳細を確認し、作成とデプロイを選択します。

   結果: サービスが正常に作成されると、コンソールにサービスダッシュボードが表示され、新しいサービスの概要が表示されます。



5. サービスが実行されていることを確認します。

   a. サービスダッシュボードページで、サービスのステータスが実行中になるまで待ちます。

   b. デフォルトのドメイン値を選択します。これは、サービスのウェブサイトへの URL です。

   c. ウェブサイトを使用して、正しく実行されていることを確認します。

App Runner API または を使用してイメージからサービスを作成する AWS CLI

App Runner API または を使用してサービスを作成するには AWS CLI、CreateService API アクションを呼び出します。

サービスの作成は、呼び出しが を示すサービスオブジェクトで成功したレスポンスを返した場合に開始されます`"Status": "CREATING"`。

呼び出しの例については、 AWS App Runner API リファレンスの「ソースイメージリポジトリサービスの作成」を参照してください。

失敗した App Runner サービスの再構築

App Runner サービスの作成時に作成失敗エラーが表示された場合は、次のいずれかを実行できます。

- の手順に従って、エラーの原因the section called “サービスの作成に失敗しました”を特定します。
- ソースまたは設定でエラーが見つかった場合は、必要な変更を加えてからサービスを再構築します。
- App Runner の一時的な問題によりサービスが失敗した場合、ソースや設定を変更せずに、失敗したサービスを再構築します。

失敗したサービスは、App Runner コンソールまたは App Runner API または AWS CLI を使用して再構築できます。

App Runner コンソールを使用した失敗した App Runner サービスの再構築

Rebuild with updates

サービスの作成は、さまざまな理由で失敗する可能性があります。この場合、サービスを再構築する前に、問題の根本原因を特定して修正することが重要です。詳細については、「the section called “サービスの作成に失敗しました”」を参照してください。

更新で失敗したサービスを再構築するには

1. サービスページの 設定 タブに移動し、編集 を選択します。

   このページに概要パネルが開き、すべての更新のリストが表示されます。
2. 必要な変更を行い、概要パネルで確認します。
3. 保存して再構築を選択します。

   サービスページのログタブで進行状況をモニタリングできます。

Rebuild without updates

一時的な問題によりサービスの作成が失敗した場合、ソースまたは設定を変更せずにサービスを再構築できます。

更新なしで失敗したサービスを再構築するには

- サービスページの右上隅にある再構築を選択します。

  サービスページのログタブで進行状況をモニタリングできます。
- サービスを再度作成できない場合は、「」のトラブルシューティング手順に従ってくださいthe section called “サービスの作成に失敗しました”。必要な変更を加え、サービスを再構築します。

App Runner API または を使用した失敗した App Runner サービスの再構築 AWS CLI

Rebuild with updates

失敗したサービスを再構築するには：

1. the section called “サービスの作成に失敗しました” 「」の手順に従って、エラーの原因を見つけます。
2. ブランチ、ソースリポジトリのイメージ、またはエラーの原因となった設定に必要な変更を加えます。
3. 新しいソースコードリポジトリまたはソースイメージリポジトリパラメータを使用して UpdateService API アクションを呼び出して再構築します。App Runner は、ソースコードリポジトリから最新のコミットを取得します。

Example 更新による再構築

次の例では、イメージベースのサービスのソース設定が更新されています。の値は に変更`Port`されます`80`。

イメージベースの App Runner サービスの `input.json` ファイルの更新

```
{
  "ServiceArn": "arn:aws:apprunner:us-east-1:123456789012:service/python-
app/8fe1e10304f84fd2b0df550fe98a71fa",
  "SourceConfiguration": {
    "ImageRepository": {
      "ImageConfiguration": {
        "Port": "80"
      }
```

```
    }
  }
}
```

`UpdateService` API アクションを呼び出します。

```
aws apprunner update-service
--cli-input-json file://input.json
```

Rebuild without updates

App Runner API または を使用して失敗したサービスを再構築するには AWS CLI、サービスのソースまたは設定を変更せずに UpdateService API アクションを呼び出します。App Runner の一時的な問題によりサービスの作成が失敗した場合にのみ、更新せずに再構築することを選択します。

App Runner への新しいアプリケーションバージョンのデプロイ

でサービスを作成するときは AWS App Runner、コンテナイメージまたはソースリポジトリなどのアプリケーションソースを設定します。App Runner は、サービスを実行するためのリソースをプロビジョニングし、そのリソースにアプリケーションをデプロイします。

このトピックでは、新しいバージョンが利用可能になったときにアプリケーションソースを App Runner サービスに再デプロイする方法について説明します。これは、イメージリポジトリの新しいイメージバージョンでも、コードリポジトリの新しいコミットでもかまいません。App Runner には、自動と手動の 2 つのデプロイ方法があります。

デプロイ方法

App Runner には、アプリケーションのデプロイの開始方法を制御するための以下の方法が用意されています。

自動デプロイ

サービスの継続的な統合とデプロイ (CI/CD) 動作が必要な場合は、自動デプロイを使用します。App Runner は、イメージまたはコードリポジトリの変更をモニタリングします。

イメージリポジトリ – 新しいイメージバージョンをイメージリポジトリにプッシュするか、コードリポジトリに新しいコミットをプッシュするたびに、App Runner はユーザー側でそれ以上のアクションを行わずに、自動的にそれをサービスにデプロイします。

コードリポジトリ – ソースディレクトリに変更を加えるコードリポジトリに新しいコミットをプッシュするたびに、App Runner はリポジトリ全体をデプロイします。ソースディレクトリの変更のみが自動デプロイをトリガーするため、ソースディレクトリの場所が自動デプロイの範囲にどのように影響するかを理解することが重要です。

- 最上位ディレクトリ (リポジトリルート) — サービスの作成時にソースディレクトリに設定されたデフォルト値です。ソースディレクトリがこの値に設定されている場合、リポジトリ全体がソースディレクトリ内にあることを意味します。したがって、ソースリポジトリにプッシュするすべてのコミットは、この場合はデプロイをトリガーします。
- リポジトリルートではないディレクトリパス (デフォルト以外) – ソースディレクトリ内でプッシュされた変更のみが自動デプロイをトリガーするため、ソースディレクトリにないリポジトリにプッシュされた変更は自動デプロイをトリガーしません。したがって、手動デプロイを使用して、ソースディレクトリの外部にプッシュする変更をデプロイする必要があります。

> **Note**
>
> App Runner は、Amazon ECR Public イメージ、およびサービスが存在するアカウントとは異なる AWS アカウントに属する Amazon ECR リポジトリ内のイメージの自動デプロイをサポートしていません。

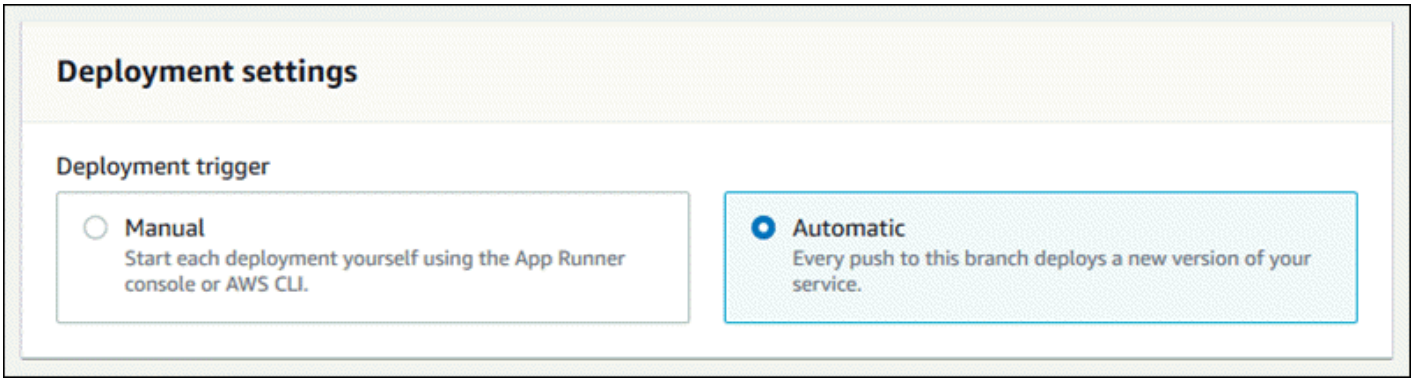
手動デプロイ

サービスへの各デプロイを明示的に開始する場合は、手動デプロイを使用します。サービス用に設定したリポジトリにデプロイする新しいバージョンがある場合は、デプロイを開始します。詳細については、「the section called “手動デプロイ”」を参照してください。

> **Note**
>
> 手動デプロイを実行すると、App Runner は完全なリポジトリからソースをデプロイします。

サービスのデプロイ方法は、次の方法で設定できます。

- コンソール – 作成する新しいサービスまたは既存のサービスについては、ソースとデプロイ設定ページのデプロイ設定セクションで、手動または自動を選択します。



- API または AWS CLI – CreateService または UpdateService アクションの呼び出しで、手動デプロイ`False`の場合は SourceConfiguration パラメータ`AutoDeploymentsEnabled`のメンバーを に設定し、自動デプロイ`True`の場合は に設定します。

> **自動デプロイと手動デプロイの比較**
>
> 自動デプロイと手動デプロイの両方が同じ結果になります。どちらの方法でもリポジトリ全体がデプロイされます。
> 2 つの方法の違いは、トリガーメカニズムです。
>
> - 手動デプロイは、コンソールからのデプロイ、 の呼び出し AWS CLI、または App Runner API の呼び出しによってトリガーされます。以下の手動デプロイセクションでは、これらの手順について説明します。
> - 自動デプロイは、ソースディレクトリの内容内の変更によってトリガーされます。

手動デプロイ

手動デプロイでは、サービスへの各デプロイを明示的に開始する必要があります。新しいバージョンのアプリケーションイメージまたはコードをデプロイする準備ができたら、以下のセクションを参照して、 コンソールと API を使用してデプロイを実行する方法を確認できます。

> **Note**
>
> 手動デプロイを実行すると、App Runner は完全なリポジトリからソースをデプロイします。

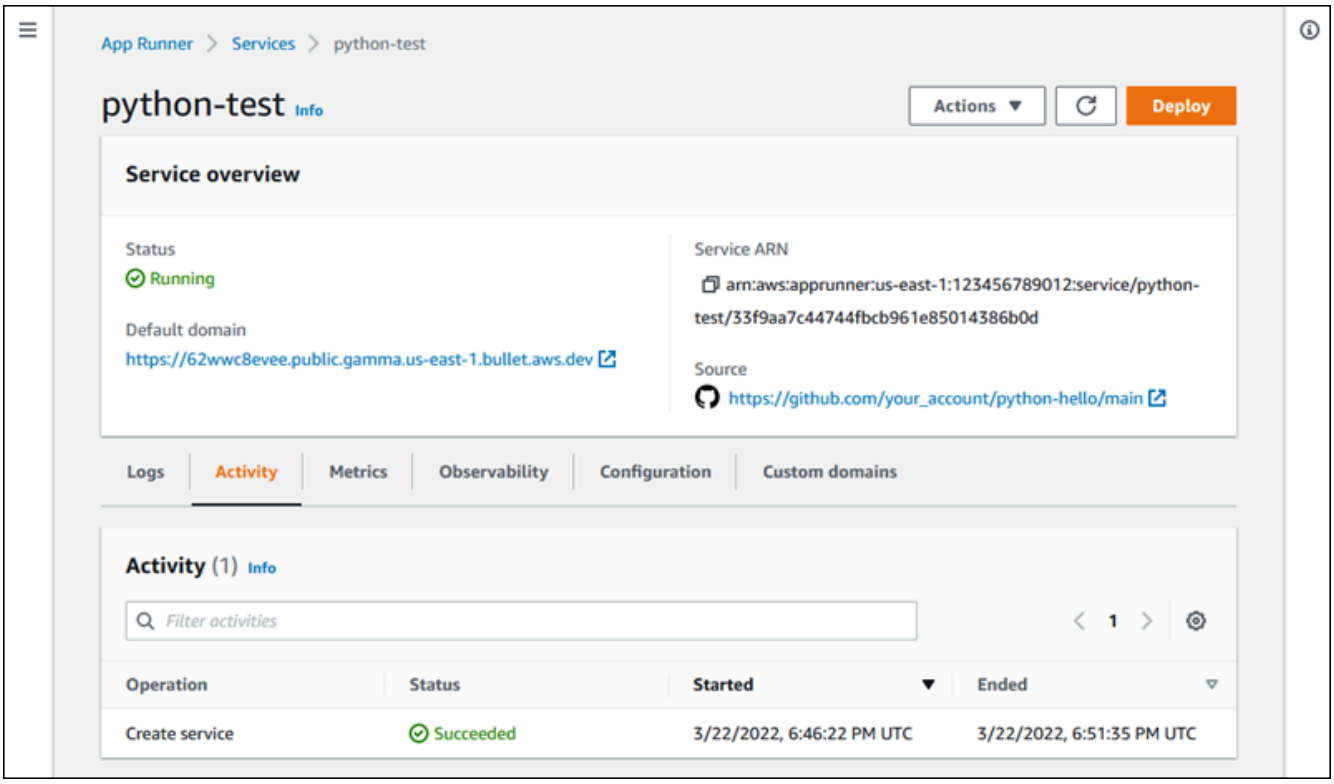
次のいずれかの方法を使用して、アプリケーションのバージョンをデプロイします。

App Runner console

App Runner コンソールを使用してデプロイするには

1. App Runner コンソールを開き、リージョンリストで を選択します AWS リージョン。
2. ナビゲーションペインで、サービスを選択し、App Runner サービスを選択します。

   コンソールには、サービスダッシュボードにサービスの概要が表示されます。



3. [デプロイ] を選択します。

   結果: 新しいバージョンのデプロイが開始されます。サービスダッシュボードページで、サービスのステータスが進行中のオペレーションに変わります。
4. デプロイが終了するのを待ちます。サービスダッシュボードページで、サービスのステータスが実行中に戻ります。
5. デプロイが成功したことを確認するには、サービスダッシュボードページで、デフォルトのドメイン値を選択します。これはサービスのウェブサイトへの URL です。ウェブアプリケーションを検査または操作し、バージョンの変更を確認します。

> **Note**
>
> App Runner アプリケーションのセキュリティを強化するために、*.awsapprunner.com ドメインはパブリックサフィックスリスト (PSL) に登録されています。セキュリティを強化するために、App Runner アプリケーションのデフォルトのドメイン名で機密 Cookie を設定する必要がある場合は、`__Host-`プレフィックス付きの Cookie を使用することをお勧めします。このプラクティスは、クロスサイトリクエストフォージェリ (CSRF) 攻撃からドメインを防ぐ際に役立ちます。詳細については、Mozilla 開発者ネットワークの「Set-Cookie」ページを参照してください。

App Runner API or AWS CLI

App Runner API または を使用してデプロイするには AWS CLI、StartDeployment API アクションを呼び出します。渡す唯一のパラメータは、サービス ARN です。サービスの作成時にアプリケーションソースの場所をすでに設定していると、App Runner は新しいバージョンを見つけることができます。呼び出しが成功したレスポンスを返すと、デプロイが開始されます。

App Runner サービスの設定

AWS App Runner サービスを作成するときは、さまざまな設定値を設定します。これらの設定の一部は、サービスの作成後に変更できます。その他の設定は、サービスの作成中にのみ適用でき、それ以降は変更できません。このトピックでは、App Runner API、App Runner コンソール、および App Runner 設定ファイルを使用したサービスの設定について説明します。

トピック

- App Runner API または を使用してサービスを設定する AWS CLI
- App Runner コンソールを使用してサービスを設定する
- App Runner 設定ファイルを使用してサービスを設定する
- サービスのオブザーバビリティの設定
- 共有可能なリソースを使用したサービス設定の構成
- サービスのヘルスチェックの設定

App Runner API または を使用してサービスを設定する AWS CLI

API は、サービスの作成後に変更できる設定を定義します。次のリストでは、関連するアクション、タイプ、制限について説明します。

- UpdateService アクション – 作成後に呼び出して、一部の設定を更新できます。
  - 更新可能 – `SourceConfiguration`、、`InstanceConfiguration`および`HealthCheckConfiguration`パラメータの設定を更新できます。ただし、 では`SourceConfiguration`、ソースタイプをコードからイメージ、またはその逆に切り替えることはできません。サービスの作成時に指定したのと同じリポジトリパラメータを指定する必要があります。これは `CodeRepository`または のいずれかです`ImageRepository`。

    サービスに関連付けられた個別の設定リソースの次の ARNs を更新することもできます。

    - `AutoScalingConfigurationArn`
    - `VpcConnectorArn`
  - 更新不可 – CreateService アクションで使用できる `ServiceName`および`EncryptionConfiguration`パラメータを変更することはできません。作成後に変更することはできません。UpdateService アクションには、これらのパラメータは含まれません。
  - API と ファイル – CodeConfiguration タイプの `ConfigurationSource`パラメータ (の一部としてソースコードリポジトリに使用`SourceConfiguration`) を に設定できます`Repository`。この場合、App Runner は の設定を無視し`CodeConfigurationValues`、リポジトリの設定ファイルからこれらの設定を読み取ります。`ConfigurationSource` を に設定すると`API`、App Runner は API コールからすべての設定を取得し、設定ファイルが存在する場合でも無視します。
- TagResource アクション – サービスの作成後に呼び出して、サービスにタグを追加したり、既存のタグの値を更新したりできます。
- UntagResource アクション – サービスの作成後に呼び出して、サービスからタグを削除できます。

> **Note**
>
> サービスのアウトバウンドトラフィック VPC コネクタを作成すると、次のサービス起動プロセスで 1 回限りのレイテンシーが発生します。この設定は、新しいサービスの作成時または作成後にサービスの更新で設定できます。詳細については、このガイド1 回限りのレイテンシーの「App Runner を使用したネットワーク」の章の「」を参照してください。

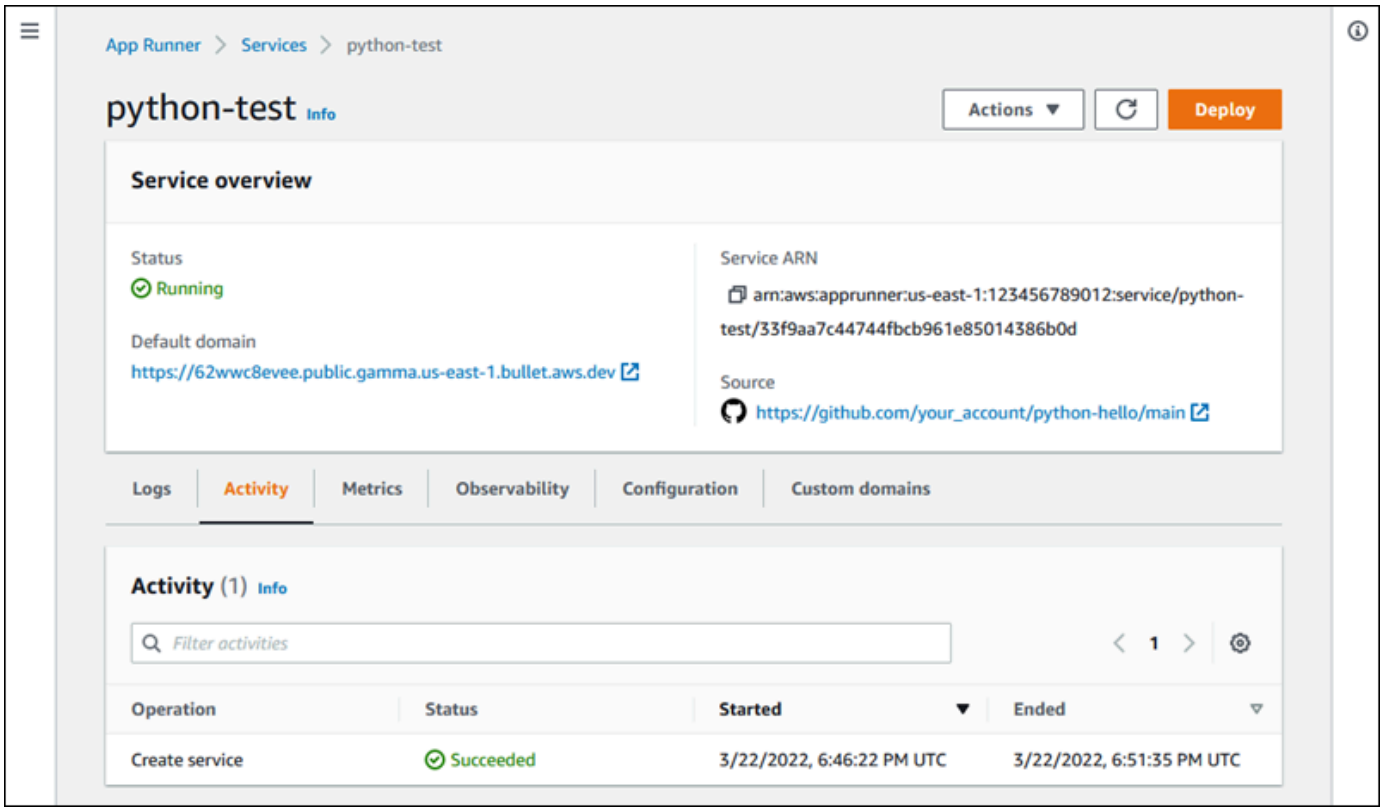
App Runner コンソールを使用してサービスを設定する

コンソールは App Runner API を使用して設定の更新を適用します。前のセクションで定義した API が課す更新ルールによって、 コンソールを使用して設定できる内容が決まります。サービスの作成時に使用可能な一部の設定は、後で変更することはできません。さらに、設定ファイルを使用する場合、追加の設定はコンソールで非表示になり、App Runner はファイルから読み取ります。

サービスを設定するには

1. App Runner コンソールを開き、リージョンリストで を選択します AWS リージョン。
2. ナビゲーションペインで、サービスを選択し、App Runner サービスを選択します。

   コンソールには、サービスダッシュボードにサービスの概要が表示されます。



3. サービスダッシュボードページで、設定タブを選択します。

   結果: コンソールには、ソースとデプロイ、ビルドの設定、サービスの設定の各セクションにサービスの現在の設定が表示されます。
4. 任意のカテゴリの設定を更新するには、編集 を選択します。
5. 設定の編集ページで、必要な変更を加え、変更の保存を選択します。

> **Note**
>
> サービスのアウトバウンドトラフィック VPC コネクタを作成すると、次のサービス起動プロセスで 1 回限りのレイテンシーが発生します。この設定は、新しいサービスの作成時または作成後にサービスの更新で設定できます。詳細については、このガイド1 回限りのレイテンシーの「Networking with App Runner」の章の「」を参照してください。

App Runner 設定ファイルを使用してサービスを設定する

App Runner サービスを作成または更新するときに、ソースリポジトリの一部として指定した設定ファイルから一部の設定を読み取るように App Runner に指示できます。これにより、ソース管理対象のソースコードに関連する設定を、コード自体とともに管理できます。設定ファイルには、コンソールまたは API を使用して設定できない特定の詳細設定も用意されています。詳細については、「App Runner 設定ファイル」を参照してください。

> **Note**
>
> サービスのアウトバウンドトラフィック VPC コネクタを作成すると、次のサービス起動プロセスで 1 回限りのレイテンシーが発生します。この設定は、新しいサービスの作成時または作成後にサービスの更新で設定できます。詳細については、このガイド1 回限りのレイテンシーの「Networking with App Runner」の章の「」を参照してください。

サービスのオブザーバビリティの設定

AWS App Runner は複数の AWS サービスと統合され、App Runner サービス用の広範なオブザーバビリティツールスイートを提供します。詳細については、「オブザーバビリティ」を参照してください。

App Runner は、オブザーバビリティ機能を有効にし、 ObservabilityConfiguration と呼ばれる共有可能なリソースを使用して動作を設定することをサポートしています。サービスを作成または更新するときに、オブザーバビリティ設定リソースを指定できます。App Runner コンソールは、新しい App Runner サービスを作成するときに自動的に作成します。オブザーバビリティ設定の提供はオプションです。指定しない場合、App Runner はデフォルトのオブザーバビリティ設定を提供します。

1 つのオブザーバビリティ設定を複数の App Runner サービス間で共有して、オブザーバビリティ動作を同じにすることができます。詳細については、「the section called “設定リソース”」を参照してください。

オブザーバビリティ設定を使用して、次のオブザーバビリティ機能を設定できます。

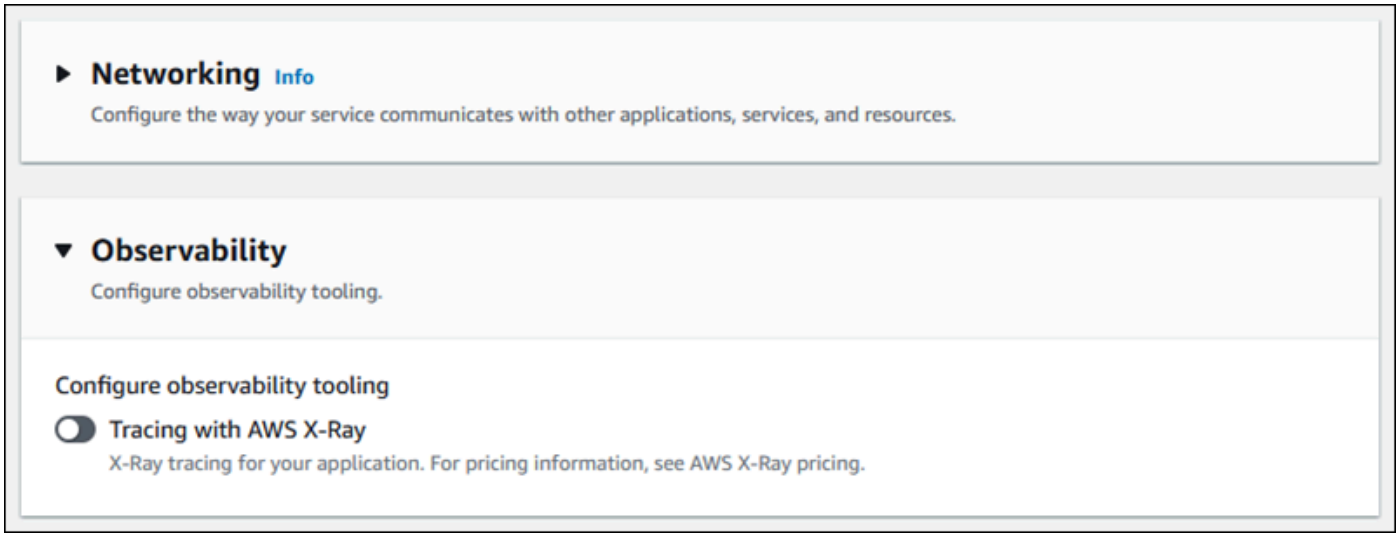
- トレース設定 – アプリケーションが処理するリクエストと、アプリケーションが行うダウンストリーム呼び出しをトレースするための設定。トレースの詳細については、「the section called “トレース (X-Ray)”」を参照してください。

オブザーバビリティの管理

次のいずれかの方法を使用して、App Runner サービスのオブザーバビリティを管理します。

App Runner console

App Runner コンソールを使用してサービスを作成する場合、または後でその設定を更新する場合は、サービスのオブザーバビリティ機能を設定できます。コンソールページのオブザーバビリティ設定セクションを探します。



App Runner API or AWS CLI

CreateService または UpdateService App Runner API アクションを呼び出すときに、`ObservabilityConfiguration`パラメータオブジェクトを使用してオブザーバビリティ機能を有効にし、サービスのオブザーバビリティ設定リソースを指定できます。

次の App Runner API アクションを使用して、オブザーバビリティ設定リソースを管理します。

- CreateObservabilityConfiguration – 新しいオブザーバビリティ設定または既存の設定へのリビジョンを作成します。
- ListObservabilityConfigurations – に関連付けられているオブザーバビリティ設定のリスト AWS アカウントと概要情報を返します。
- DescribeObservabilityConfiguration – オブザーバビリティ設定の完全な説明を返します。
- DeleteObservabilityConfiguration – オブザーバビリティ設定を削除します。特定のリビジョンまたは最新のアクティブなリビジョンを削除できます。のオブザーバビリティ設定クォータに達した場合は、不要なオブザーバビリティ設定を削除する必要がある場合があります AWS アカウント。

共有可能なリソースを使用したサービス設定の構成

一部の機能では、 AWS App Runner サービス間で設定を共有するのが理にかなっています。たとえば、一連のサービスに同じ自動スケーリング動作を持たせたい場合があります。または、すべてのサービスに対して同じオブザーバビリティ設定が必要な場合があります。App Runner では、個別の共有可能なリソースを使用して設定を共有できます。機能の一連の設定を定義するリソースを作成し、この設定リソースの Amazon リソースネーム (ARN) を 1 つ以上の App Runner サービスに提供します。

App Runner は、以下の機能に共有可能な設定リソースを実装します。

- Auto scaling
- 可観測性
- VPC アクセス

これらの各機能のドキュメントページには、使用可能な設定と管理手順に関する情報が表示されます。

個別の設定リソースを使用する機能は、いくつかの設計特性と考慮事項を共有します。

- リビジョン – 一部の設定リソースにはリビジョンを含めることができます。自動スケーリングとオブザーバビリティは、リビジョンを使用する 2 つの設定リソースの例です。このような場合、各設定には名前と数値リビジョンがあります。設定の複数のリビジョンには、同じ名前と異なるリビジョン番号があります。シナリオごとに異なる設定名を使用できます。名前ごとに複数のリビジョンを追加して、特定のシナリオの設定を微調整できます。

名前で作成した最初の設定は、リビジョン番号 1 を取得します。同じ名前の後続の設定では、リビジョン番号が連続して取得されます (2 で始まる) 。App Runner サービスは、特定の設定リビジョンまたは最新の設定リビジョンに関連付けることができます。

- 共有 – 1 つの設定リソースを複数の App Runner サービス間で共有できます。これは、これらのサービス全体で同じ設定を維持する場合に便利です。特に、リソースがリビジョンをサポートしている場合は、設定の最新リビジョンを使用するように複数のサービスを設定できます。これを行うには、リビジョンではなく、設定名のみを指定します。この方法で設定したサービスはいずれも、サービスの更新時に設定の更新を受け取ります。設定の変更の詳細については、「」を参照してくださいthe section called “設定”。
- リソース管理 – App Runner を使用して設定を作成および削除できます。設定を直接更新することはできません。代わりに、リビジョンをサポートするリソースの場合、既存の設定名に新しいリビジョンを作成して、設定を効果的に更新できます。

> **Note**
>
> 自動スケーリングでは、App Runner コンソールと App Runner API の両方を使用して設定と複数のリビジョンを作成できます。App Runner コンソールと App Runner API の両方が、設定とリビジョンを削除することもできます。詳細については、「App Runner 自動スケーリングの管理」を参照してください。
> オブザーバビリティ設定など、他の設定タイプでは、App Runner コンソールで作成できる設定は 1 つのリビジョンのみです。さらにリビジョンを作成し、設定を削除するには、App Runner API を使用する必要があります。

- リソースクォータ – 各設定リソースに対して設定できる一意の設定名とリビジョンの数にクォータが設定されています AWS リージョン。これらのクォータに達した場合は、さらに作成する前に、設定名またはそのリビジョンの一部を削除する必要があります。自動スケーリング設定リビジョンの場合は、App Runner コンソールまたは App Runner API を使用して削除できます。詳細については、「App Runner 自動スケーリングの管理」を参照してください。他のリソースを削除するには、App Runner API を使用する必要があります。クォータの詳細については、「the section called “App Runner リソースクォータ”」を参照してください。
- リソースコストなし – 設定リソースの作成に追加コストは発生しません。機能自体のコストが発生する場合があります (たとえば、X-Ray トレースを有効にすると通常の AWS X-Ray コストが課金されます) 。ただし、App Runner サービスの機能を設定する App Runner 設定リソースのコストは発生しません。

サービスのヘルスチェックの設定

AWS App Runner は、ヘルスチェックを実行してサービスの状態をモニタリングします。デフォルトのヘルスチェックプロトコルは TCP です。App Runner は、サービスに割り当てられたドメインに ping を実行します。または、ヘルスチェックプロトコルを HTTP に設定することもできます。App Runner は、ウェブアプリケーションにヘルスチェック HTTP リクエストを送信します。

ヘルスチェックに関連する設定をいくつか設定できます。次の表に、ヘルスチェックの設定とそのデフォルト値を示します。

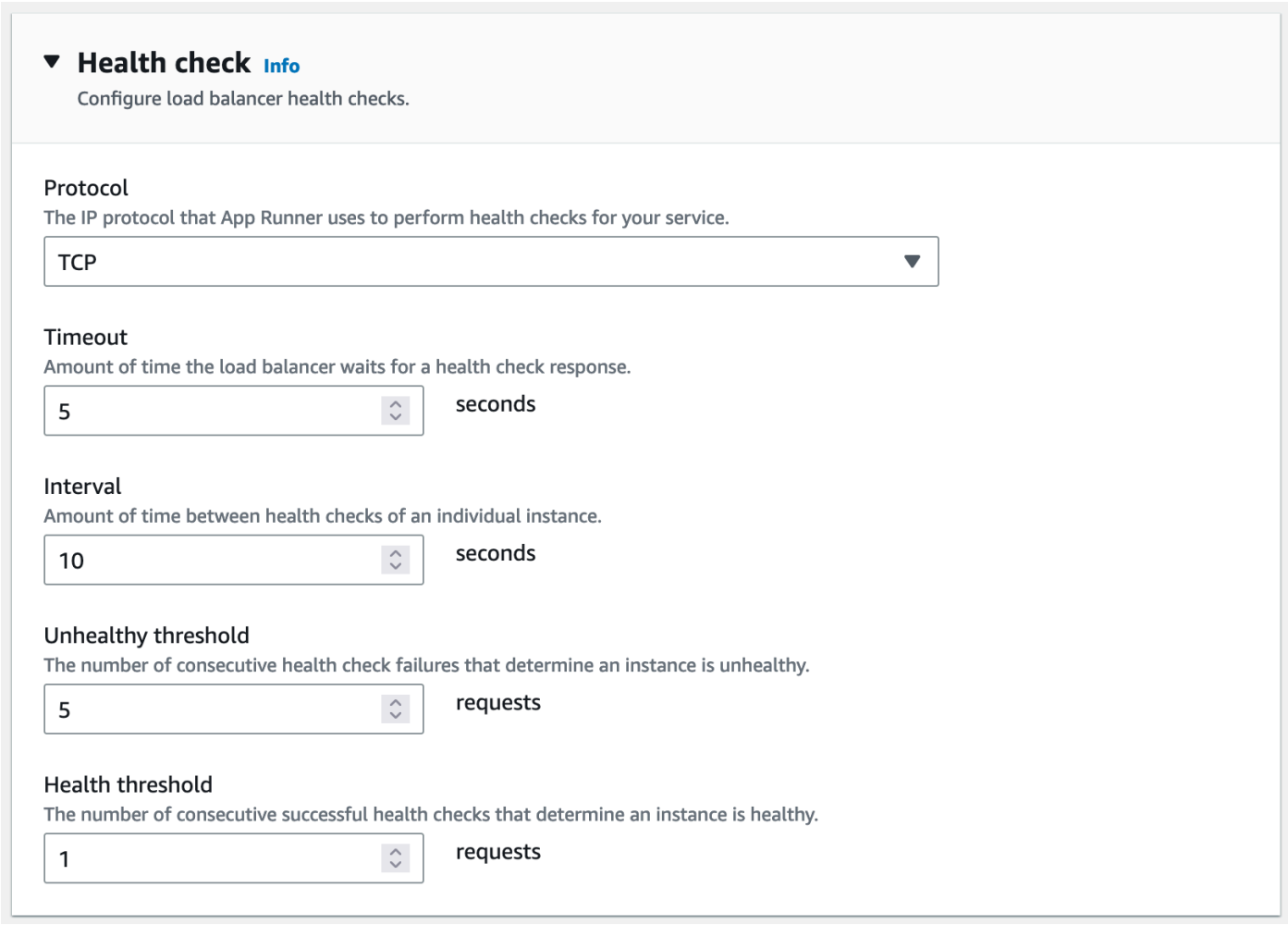
設定	説明	デフォルト
プロトコル	App Runner がサービスのヘルスチェックを実行するために使用する IP プロトコル。 プロトコルを に設定するとTCP、App Runner はアプリケーションがリッスンしているポートでサービスに割り当てられたデフォルトのドメインに ping を実行します。 プロトコルを に設定するとHTTP、App Runner は設定されたパスにヘルスチェックリクエストを送信します。	TCP
パス	App Runner が HTTP ヘルスチェックリクエストを送信する URL。HTTP チェックにのみ適用されます。	/
間隔	ヘルスチェックの間隔 (秒)。	5
タイムアウト	ヘルスチェックの応答が失敗したと判断されるまでの時間 (秒)。	2
正常なしきい値	App Runner がサービスが正常であると判断するために成功する必要がある連続チェックの数。	1
異常なしきい値	App Runner がサービスが異常であると判断するために失敗する必要がある連続チェックの数。	5

ヘルスチェックを設定する

次のいずれかの方法を使用して、App Runner サービスのヘルスチェックを設定します。

App Runner console

App Runner コンソールを使用して App Runner サービスを作成する場合、または後でその設定を更新する場合は、ヘルスチェック設定を設定できます。コンソールの詳細な手順については、the section called “作成”「」および「」を参照してくださいthe section called “設定”。いずれの場合も、コンソールページのヘルスチェック設定セクションを探します。



App Runner API or AWS CLI

CreateService または UpdateService API アクションを呼び出すときは、`HealthCheckConfiguration`パラメータを使用してヘルスチェック設定を指定できます。

パラメータの構造の詳細については、 AWS App Runner API リファレンスのHealthCheckConfiguration」を参照してください。

App Runner 接続の管理

でサービスを作成するときは AWS App Runner、アプリケーションソース、つまりプロバイダーに保存されているコンテナイメージまたはソースリポジトリを設定します。App Runner は、プロバイダーとの認証および認可された接続を確立する必要があります。その後、App Runner はリポジトリを読み取ってサービスにデプロイできます。App Runner は、 に保存されているコードにアクセスするサービスを作成するときに接続確立を必要としません AWS アカウント。

App Runner は、接続と呼ばれるリソースの接続情報を維持します。App Runner コンソールとこのガイドでは、接続を接続アカウントと呼びます。App Runner では、サードパーティーの接続情報を必要とするサービスを作成するときに、接続リソースが必要です。以下は、接続に関する重要な情報です。

- プロバイダー – App Runner は現在、GitHub または Bitbucket との接続リソースを必要とします。
- 共有 – 接続リソースを使用して、同じリポジトリプロバイダーアカウントを使用する複数の App Runner サービスを作成できます。
- リソース管理 – App Runner では、接続を作成および削除できます。ただし、既存の接続を変更することはできません。
- リソースクォータ – 接続リソースには、各 AWS アカウント の に関連付けられたクォータが設定されています AWS リージョン。このクォータに達した場合は、新しいプロバイダーアカウントに接続する前に接続を削除する必要がある場合があります。次のセクション「」で説明するように、App Runner コンソールまたは API を使用して接続を削除できますthe section called “接続の管理”。詳細については、「the section called “App Runner リソースクォータ”」を参照してください。

接続の管理

次のいずれかの方法を使用して App Runner 接続を管理します。

App Runner console

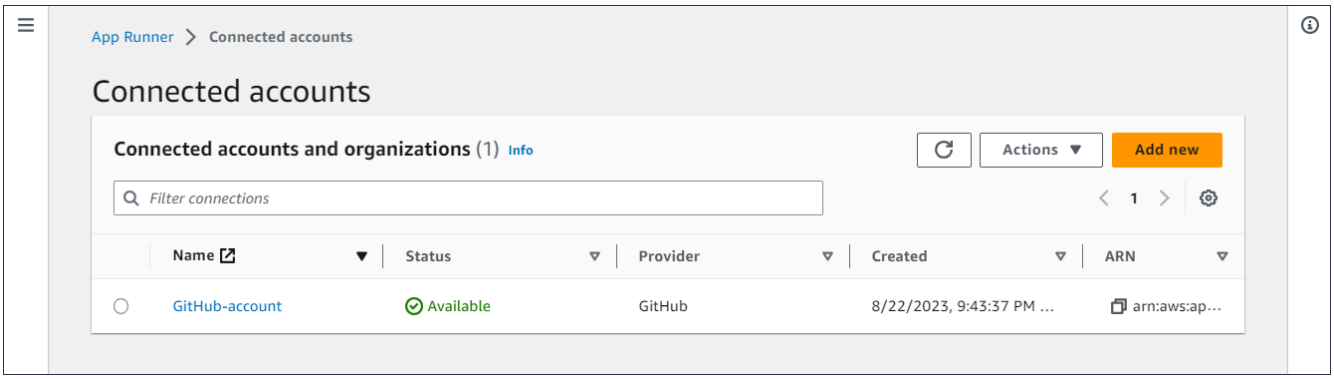
App Runner コンソールを使用してサービスを作成する場合は、接続の詳細を指定します。接続リソースを明示的に作成する必要はありません。コンソールでは、以前に接続した GitHub または Bitbucket アカウントに接続するか、新しいアカウントに接続するかを選択できます。必要に応じて、App Runner が接続リソースを作成します。新しい接続の場合、一部のプロバイダーでは、接続を使用する前に認証ハンドシェイクを完了する必要があります。コンソールでこのプロセスを実行します。

コンソールには、既存の接続を管理するページもあります。サービスの作成時に認証ハンドシェイクを実行しなかった場合は、接続の認証ハンドシェイクを完了できます。使用しなくなった接続を削除することもできます。次の手順は、リポジトリプロバイダー接続を管理する方法を示しています。

アカウントの接続を管理するには

1. App Runner コンソールを開き、リージョンリストで を選択します AWS リージョン。
2. ナビゲーションペインで、接続されたアカウントを選択します。

   次に、コンソールにアカウントのリポジトリプロバイダー接続のリストが表示されます。



3. リスト上の任意の接続を使用して、次のいずれかのアクションを実行できるようになりました。
   - GitHub/Bitbucket アカウントまたは組織を開く – 接続の名前を選択します。
   - 認証ハンドシェイクの完了 – 接続を選択し、アクションメニューからハンドシェイクの完了を選択します。コンソールでは、認証ハンドシェイクプロセスについて説明します。
   - 接続の削除 – 接続を選択し、アクションメニューから削除を選択します。削除プロンプトの指示に従います。

App Runner API or AWS CLI

次の App Runner API アクションを使用して接続を管理できます。

- CreateConnection – リポジトリプロバイダーアカウントへの接続を作成します。接続を作成したら、App Runner コンソールを使用して認証ハンドシェイクを手動で完了する必要があります。このプロセスについては、前のセクションで説明します。
- ListConnections – に関連付けられている App Runner 接続のリストを返します AWS アカウント。

- DeleteConnection – 接続を削除します。の接続クォータに達した場合は、不要な接続を削除する必要がある場合があります AWS アカウント。

App Runner 自動スケーリングの管理

AWS App Runner は、App Runner アプリケーションのコンピューティングリソース、特にインスタンスを自動的にスケールアップまたはスケールダウンします。自動スケーリングは、トラフィックが重い場合に適切なリクエスト処理を提供し、トラフィックが遅くなった場合にコストを削減します。

Auto Scaling 設定

いくつかのパラメータを設定して、サービスの Auto Scaling 動作を調整できます。App Runner は、AutoScalingConfiguration と呼ばれる共有可能なリソースで自動スケーリング設定を維持します。サービスに割り当てる前に、スタンドアロンの自動スケーリング設定を作成して維持できます。サービスに関連付けられたら、設定を引き続き維持できます。新しいサービスの作成中または既存のサービスの設定中に、新しい自動スケーリング設定を作成することもできます。新しい Auto Scaling 設定が作成されたら、それをサービスに関連付けて、サービスを作成または設定するプロセスを続行できます。

命名とリビジョン

自動スケーリング設定には、名前と数値リビジョンがあります。設定の複数のリビジョンには、同じ名前と異なるリビジョン番号があります。高可用性や低コストなど、さまざまな Auto Scaling シナリオに異なる設定名を使用できます。名前ごとに複数のリビジョンを追加して、特定のシナリオの設定を微調整できます。設定ごとに最大 10 個の一意の自動スケーリング設定名と最大 5 個のリビジョンを持つことができます。制限に達し、さらに作成する必要がある場合は、その制限を削除してから別の制限を作成できます。App Runner では、デフォルトとして設定されているか、アクティブなサービスで使用されている設定を削除することはできません。クォータの詳細については、「the section called “App Runner リソースクォータ”」を参照してください。

デフォルト設定の設定

App Runner サービスを作成または更新するときに、Auto Scaling 設定リソースを指定できます。自動スケーリング設定の提供はオプションです。指定しない場合、App Runner は推奨値を含むデフォルトの自動スケーリング設定を提供します。自動スケーリング設定機能を使用すると、App Runner が提供するデフォルトを使用する代わりに、独自のデフォルトの自動スケーリング設定を設定できます。別の Auto Scaling 設定をデフォルトとして指定すると、その設定は今後作成する新しいサービスに自動的にデフォルトとして割り当てられます。新しいデフォルトの指定は、既存のサービスに以前に設定された関連付けには影響しません。

自動スケーリングによるサービスの設定

1 つの Auto Scaling 設定を複数の App Runner サービス間で共有して、サービスに同じ Auto Scaling 動作を持たせることができます。App Runner コンソールまたは App Runner API を使用して自動スケーリング設定を設定する方法の詳細については、このトピックで後述するセクションを参照してください。共有可能なリソースの詳細については、「」を参照してくださいthe section called “設定リソース”。

設定可能な設定

次の Auto Scaling 設定を構成できます。

- 最大同時実行数 – インスタンスが処理する同時リクエストの最大数。同時リクエストの数がこのクォータを超えると、App Runner はサービスをスケールアップします。
- 最大サイズ – サービスがスケールアップできるインスタンスの最大数。これは、サービスのトラフィックを同時に処理できるインスタンスの最大数です。
- 最小サイズ – App Runner がサービスにプロビジョニングできるインスタンスの最小数。サービスには、少なくともこの数のプロビジョニングされたインスタンスがあります。これらのインスタンスの一部は、トラフィックをアクティブに処理します。残りは、費用対効果の高いコンピューティングキャパシティーリザーブの一部であり、すぐにアクティブ化できます。プロビジョニングされたすべてのインスタンスのメモリ使用量に対して料金が発生します。アクティブなサブセットのみの CPU 使用率に対して料金が発生します。

> **Note**
>
> vCPU リソース数は、App Runner がサービスに提供できるインスタンスの数を決定します。これは、 AWS Fargate サービスに存在する Fargate オンデマンド vCPU リソース数の調整可能なクォータ値です。アカウントの vCPU クォータ設定を表示したり、クォータの引き上げをリクエストしたりするには、 の Service Quotas コンソールを使用します AWS Management Console。詳細については、「Amazon Elastic Container Service デベロッパーガイド」の「サービスAWS Fargate クォータ」を参照してください。

サービスの自動スケーリングを管理する

次のいずれかの方法を使用して、App Runner サービスの自動スケーリングを管理します。

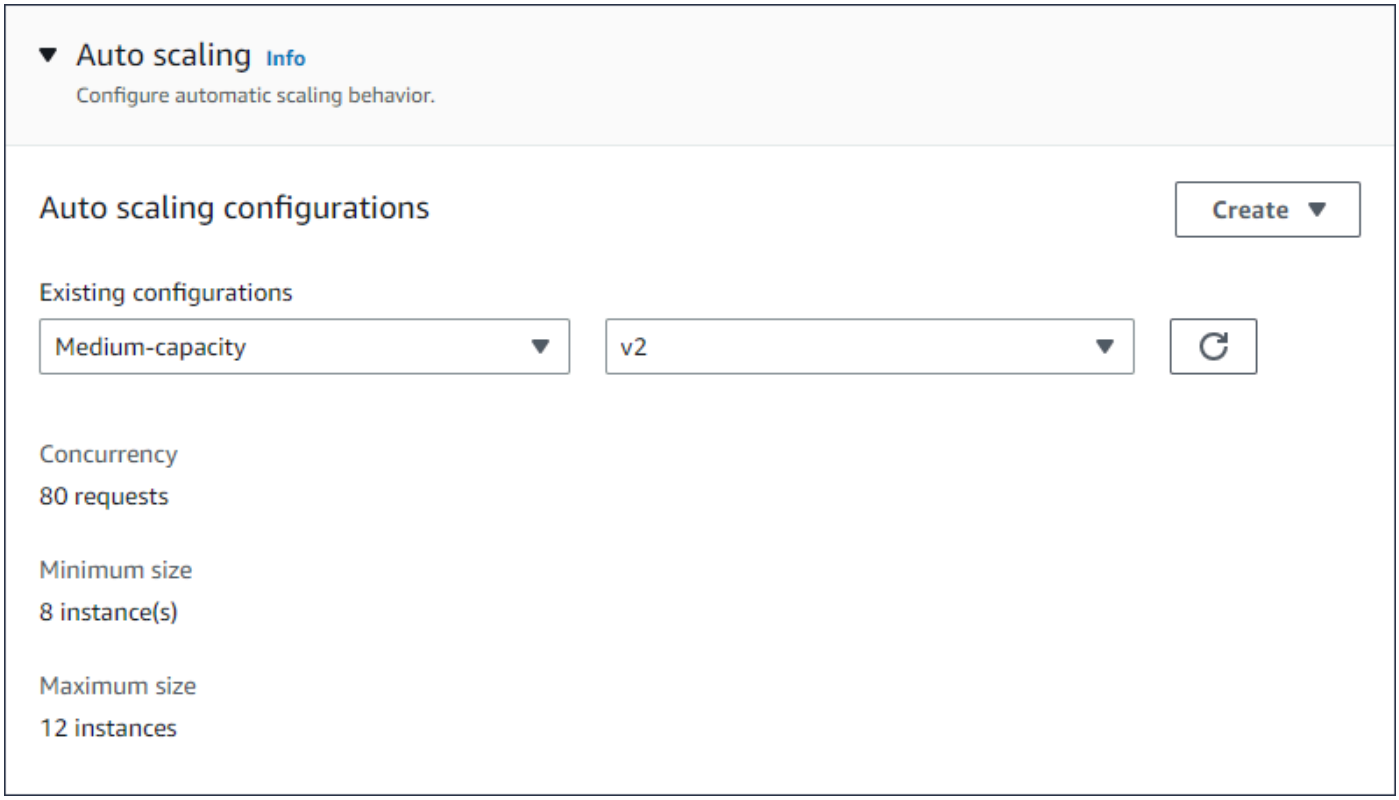
App Runner console

App Runner コンソールを使用してサービスを作成する場合、またはサービス設定を更新する場合は、自動スケーリング設定を指定できます。

> **Note**
>
> サービスに関連付けられている自動スケーリング設定またはリビジョンを変更すると、サービスが再デプロイされます。

Auto Scaling 設定ページには、サービスの Auto Scaling を設定するためのオプションがいくつか用意されています。

- 既存の設定とリビジョンを割り当てるには – 既存の設定ドロップダウンから値を選択します。最新のリビジョンバージョンは、隣接するドロップダウンでデフォルトになります。選択したい別のリビジョンが存在する場合は、リビジョンのドロップダウンから選択します。リビジョンバージョンの設定値が表示されます。
- 新しい自動スケーリング設定を作成して割り当てるには – 作成メニューから新しい ASC の作成を選択します。これにより、カスタム自動スケーリング設定の追加ページが起動します。自動スケーリングパラメータの設定名と値を入力します。次に、[追加] をクリックします。App Runner は新しい Auto Scaling 設定リソースを作成し、新しい設定を選択して表示した状態で Auto Scaling セクションに戻ります。
- 新しいリビジョンを作成して割り当てるには – まず、既存の設定ドロップダウンから設定名を選択します。次に、作成メニューから ASC リビジョンの作成を選択します。これにより、カスタム自動スケーリング設定の追加ページが起動します。自動スケーリングパラメータの値を入力します。次に、[追加] をクリックします。App Runner は、新しい Auto Scaling 設定リビジョンを作成し、新しいリビジョンを選択して表示した状態で Auto Scaling セクションに戻ります。



App Runner API or AWS CLI

CreateService または UpdateService App Runner API アクションを呼び出すときに、`AutoScalingConfigurationArn`パラメータを使用して、サービスの Auto Scaling 設定リソースを指定できます。

次のセクションでは、Auto Scaling 設定リソースを管理するためのガイダンスを提供します。

Auto Scaling 設定リソースを管理する

次のいずれかの方法を使用して、アカウントの App Runner 自動スケーリング設定とリビジョンを管理します。

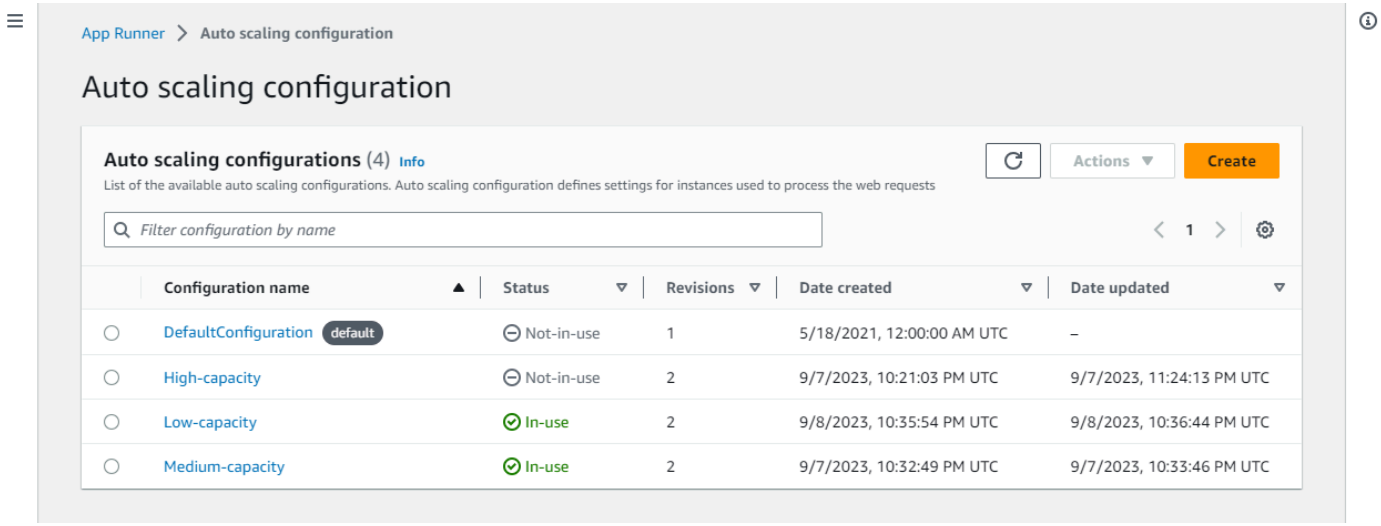
App Runner console

自動スケーリング設定を管理する

Auto Scaling 設定ページには、アカウントで設定した Auto Scaling 設定が一覧表示されます。このページで自動スケーリング設定を作成および管理し、後で 1 つ以上の App Runner サービスに割り当てることができます。

このページから次のいずれかを実行できます。

- 新しい Auto Scaling 設定を作成します。
- 既存の Auto Scaling 設定の新しいリビジョンを作成します。
- 自動スケーリング設定を削除します。
- 自動スケーリング設定をデフォルトとして設定します。



アカウントで自動スケーリング設定を管理するには

1. App Runner コンソールを開き、リージョンリストで を選択します AWS リージョン。
2. ナビゲーションペインで、Auto Scaling 設定を選択します。コンソールには、アカウントの Auto Scaling 設定のリストが表示されます。

   これで、次のいずれかを実行できます。

   - 新しい Auto Scaling 設定を作成するには、次の手順に従います。

     a. Auto Scaling 設定ページで、作成を選択します。

        自動スケーリング設定の作成ページが表示されます。

     b. 設定名、同時実行数、最小サイズ、最大サイズの値を入力します。

     c. (オプション) タグを追加する場合は、Auto new tag を選択します。次に、表示されるフィールドに名前と値を入力します (オプション) 。

     d. [作成] を選択します。

   - 既存の Auto Scaling 設定の新しいリビジョンを作成するには、次の手順に従います。

a. Auto Scaling 設定ページで、新しいリビジョンを必要とする設定の横にあるラジオボタンを選択します。次に、アクションメニューからリビジョンの作成を選択します。

   リビジョンの作成ページが表示されます。

b. で、同時実行、最小サイズ、最大サイズの値を入力します。

c. (オプション) タグを追加する場合は、Auto new tag を選択します。次に、表示されるフィールドに名前と値を入力します (オプション) 。

d. [作成] を選択します。

- 自動スケーリング設定を削除するには、次の手順に従います。

  a. Auto Scaling 設定ページで、削除する必要がある設定の横にあるラジオボタンを選択します。

  b. アクションメニューから削除を選択します。

  c. 削除を続行するには、確認ダイアログで削除を選択します。それ以外の場合は、キャンセルを選択します。

  > **Note**
  >
  > App Runner は、削除の選択がデフォルトとして設定されていないか、アクティブなサービスで現在使用されていることを検証します。

- 自動スケーリング設定をデフォルトとして設定するには、次の手順に従います。

  a. Auto Scaling 設定ページで、デフォルトとして設定する必要がある設定の横にあるラジオボタンを選択します。

  b. アクションメニューからデフォルトとして設定を選択します。

  c. App Runner が、作成したすべての新しいサービスのデフォルト設定として最新のリビジョンを使用することを示すダイアログが表示されます。確認を選択して続行します。それ以外の場合は、キャンセルを選択します。

  > **Note**
  >
  > - 自動スケーリング設定をデフォルトに設定すると、今後作成する新しいサービスにデフォルト設定として自動的に割り当てられます。

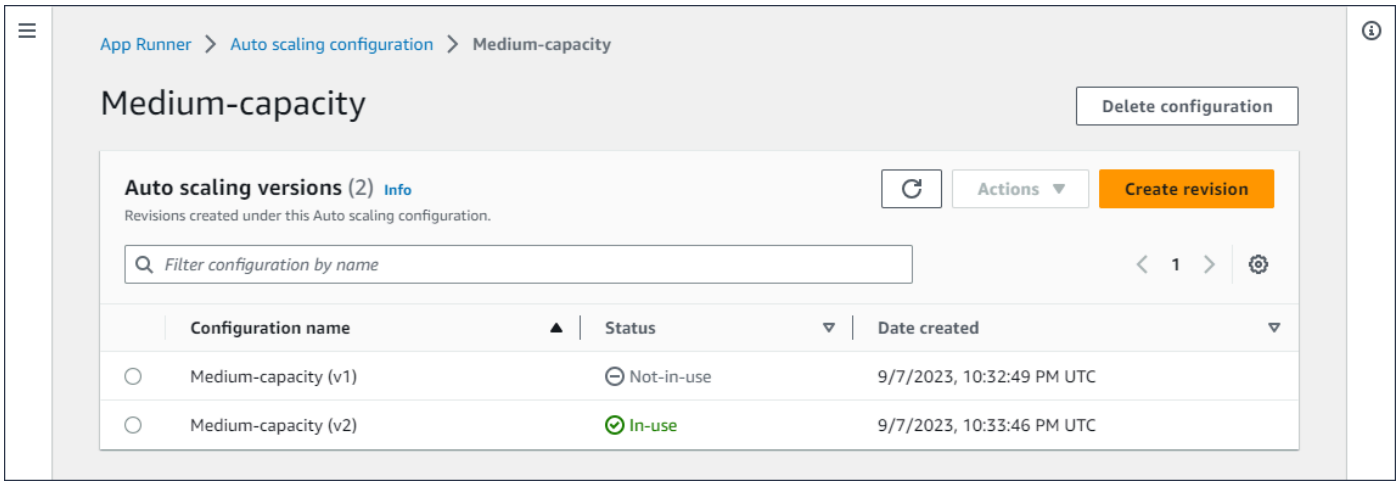
- 新しいデフォルトの指定は、既存のサービスに以前に設定された関連付けには影響しません。
- 指定されたデフォルトの自動スケーリング設定にリビジョンがある場合、App Runner は最新のリビジョンをデフォルトとして割り当てます。

リビジョンの管理

コンソールには、Auto Scaling リビジョンと呼ばれる既存の Auto Scaling リビジョンを作成および管理するためのページもあります。Auto Scaling 設定ページで設定の名前を選択して、このページにアクセスします。

Auto Scaling リビジョンページから次のいずれかを実行できます。

- 新しい Auto Scaling リビジョンを作成します。
- 自動スケーリング設定リビジョンをデフォルトとして設定します。
- リビジョンを削除します。
- 関連するすべてのリビジョンを含め、Auto Scaling 設定全体を削除します。
- リビジョンの設定の詳細を表示します。
- リビジョンに関連付けられたサービスのリストを表示します。
- リストされたサービスのリビジョンを変更します。



アカウントで Auto Scaling リビジョンを管理するには

1. App Runner コンソールを開き、リージョンリストで を選択します AWS リージョン。

2. ナビゲーションペインで、Auto Scaling 設定を選択します。コンソールには、アカウントの Auto Scaling 設定のリストが表示されます。自動スケーリング設定を管理する セクションの前の手順のセットには、このページの画面イメージが含まれています。
3. これで、特定の自動スケーリング設定をドリルダウンして、そのすべてのリビジョンを表示および管理できるようになりました。Auto Scaling 設定ペインの設定名列で、Auto Scaling 設定名を選択します。ラジオボタンではなく実際の名前を選択します。これにより、Auto Scaling リビジョンページのその設定のすべてのリビジョンのリストに移動します。
4. これで、次のいずれかを実行できます。
   - 既存の Auto Scaling 設定の新しいリビジョンを作成するには、次の手順に従います。
     a. Auto Scaling リビジョンページで、リビジョンの作成を選択します。

        リビジョンの作成ページが表示されます。
     b. 同時実行、最小サイズ、最大サイズの値を入力します。
     c. (オプション) タグを追加する場合は、Auto new tag を選択します。次に、表示されるフィールドに名前と値を入力します (オプション) 。
     d. [作成] を選択します。
   - 関連するすべてのリビジョンを含む Auto Scaling 設定全体を削除するには、次の手順に従います。
     a. ページの右上にある設定の削除を選択します。
     b. 削除を続行するには、確認ダイアログで削除を選択します。それ以外の場合は、キャンセルを選択します。

        > **Note**
        > App Runner は、削除の選択がデフォルトとして設定されていないか、アクティブなサービスで現在使用されていることを検証します。
   - 自動スケーリングリビジョンをデフォルトとして設定するには、次の手順に従います。
     a. デフォルトとして設定する必要があるリビジョンの横にあるラジオボタンを選択します。
     b. アクションメニューからデフォルトとして設定を選択します。

> **Note**
>
> - 自動スケーリング設定をデフォルトに設定すると、今後作成する新しいサービスにデフォルト設定として自動的に割り当てられます。
> - 新しいデフォルトの指定は、既存のサービスに以前に設定された関連付けには影響しません。

- リビジョンの設定の詳細を表示するには、次の手順に従います。
  - リビジョンの横にあるラジオボタンを選択します。

    ARN を含むリビジョンの設定の詳細は、下部の分割パネルに表示されます。この手順の最後にある画面イメージを参照してください。
- リビジョンに関連付けられているサービスのリストを表示するには、次の手順に従います。
  - リビジョンの横にあるラジオボタンを選択します。

    サービスパネルは、下部の分割パネルのリビジョン設定の詳細の下に表示されます。パネルには、この Auto Scaling 設定リビジョンを使用するすべてのサービスが一覧表示されます。この手順の最後にある画面イメージを参照してください。
- リストされたサービスのリビジョンを変更するには、次の手順に従います。

  a. リビジョンの横にあるラジオボタンがまだない場合は、それを選択します。

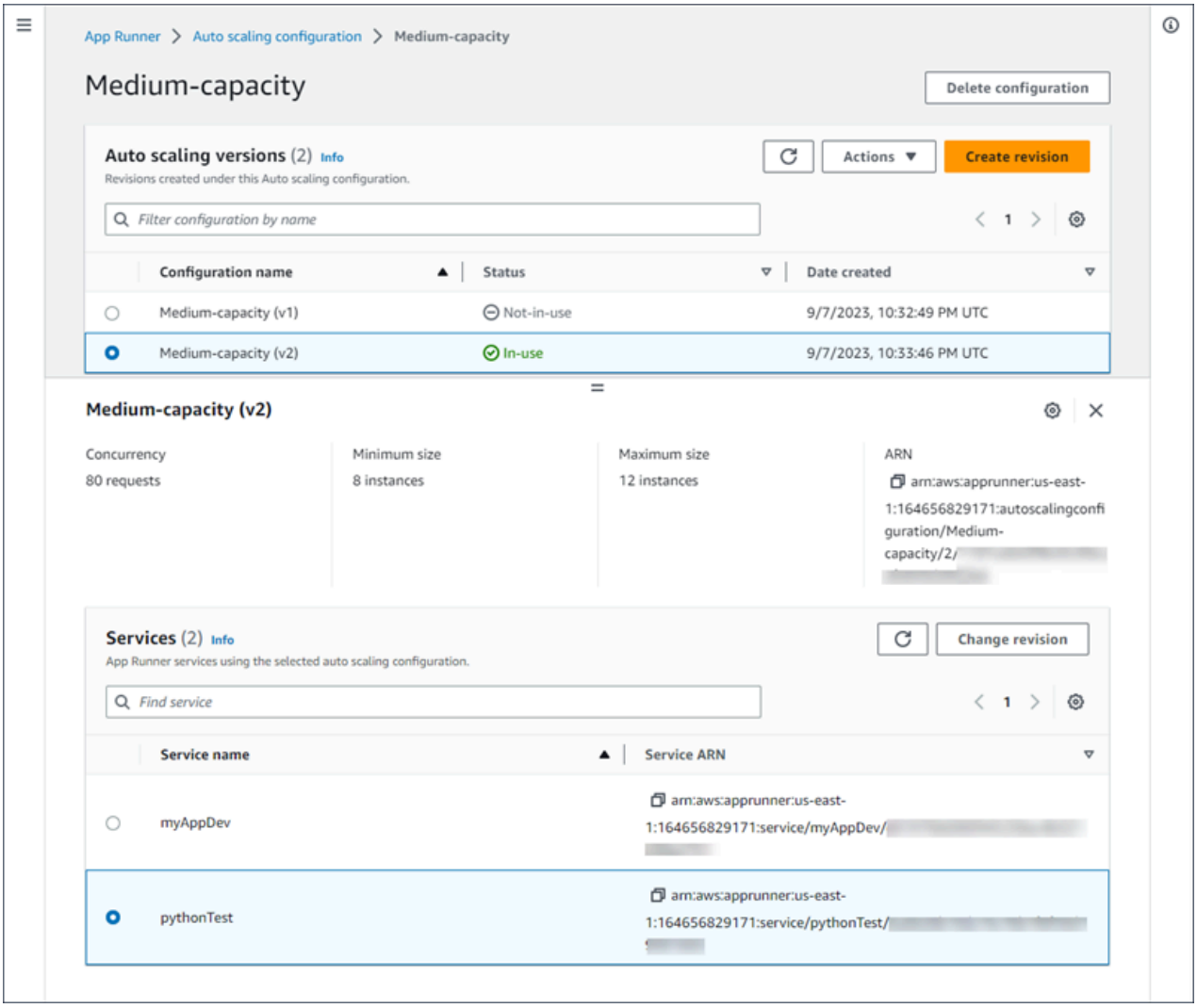
     サービスパネルは、下部の分割パネルのリビジョン設定の詳細の下に表示されます。パネルには、この Auto Scaling 設定リビジョンを使用するすべてのサービスが一覧表示されます。この手順の最後にある画面イメージを参照してください。

  b. サービスパネルで、変更するサービスの横にあるラジオボタンを選択します。次に、リビジョンの変更を選択します。

  c. ASC リビジョンの変更パネルが表示されます。ドロップダウンで使用可能なリビジョンから選択します。前に選択した Auto Scaling 設定のリビジョンのみを使用できます。別の Auto Scaling 設定に変更する必要がある場合は、前のセクションの手順に従ってくださいthe section called “サービスの自動スケーリングを管理する”。

     更新を選択して変更を続行します。それ以外の場合は、キャンセルを選択します。

> **Note**
>
> サービスに関連付けられているリビジョンを変更すると、サービスが再デプロイされます。
> 更新された関連付けを表示するには、このパネルで更新を選択する必要があります。
> 進行中のアクティビティとサービス再デプロイのステータスを確認するには、パネルのパンくずリストを使用して App Runner > サービスに移動し、サービスを選択し、サービスの概要パネルからログタブを表示します。



App Runner API or AWS CLI

次の App Runner API アクションを使用して、自動スケーリング設定リソースを管理します。

- CreateAutoScalingConfiguration – 新しい自動スケーリング設定または既存の設定へのリビジョンを作成します。
- UpdateDefaultAutoScalingConfiguration – 自動スケーリング設定をデフォルトに設定します。既存のデフォルトの自動スケーリング設定は、デフォルト以外の設定に自動的に設定されます。
- ListAutoScalingConfigurations – に関連付けられている自動スケーリング設定のリスト AWS アカウントと概要情報を返します。
- ListServicesForAutoScalingConfiguration – 自動スケーリング設定を使用して、関連する App Runner サービスのリストを返します。
- DescribeAutoScalingConfiguration – 自動スケーリング設定の完全な説明を返します。
- DeleteAutoScalingConfiguration – 自動スケーリング設定を削除します。最上位の自動スケーリング設定、1 つの特定のリビジョン、または最上位設定に関連付けられたすべてのリビジョンを削除できます。オプションの `DeleteAllRevisions`パラメータを使用して、すべてのリビジョンを削除します。の Auto Scaling 設定リソースクォータに達した場合は AWS アカウント、不要な Auto Scaling 設定を削除する必要がある場合があります。

App Runner サービスのカスタムドメイン名の管理

AWS App Runner サービスを作成すると、App Runner はそのサービスにドメイン名を割り当てます。これは、App Runner が所有する`awsapprunner.com`ドメイン内のサブドメインです。ドメイン名を使用して、 サービスで実行されているウェブアプリケーションにアクセスできます。

> **Note**
>
> App Runner アプリケーションのセキュリティを強化するために、*.awsapprunner.com ドメインはパブリックサフィックスリスト (PSL) に登録されています。セキュリティを強化するために、App Runner アプリケーションのデフォルトのドメイン名に機密 Cookie を設定する必要がある場合は、`__Host-`プレフィックス付きの Cookie を使用することをお勧めします。このプラクティスは、クロスサイトリクエストフォージェリ (CSRF) 攻撃からドメインを防ぐ際に役立ちます。詳細については、Mozilla 開発者ネットワークの「Set-Cookie」ページを参照してください。

ドメイン名を所有している場合は、App Runner サービスに関連付けることができます。App Runner が新しいドメインを検証したら、そのドメインを使用して App Runner ドメインに加えてアプリケーションにアクセスできます。最大 5 つのカスタムドメインを関連付けることができます。

> **Note**
>
> オプションで、ドメインのwwwサブドメインを含めることができます。ただし、これは現在 API でのみサポートされています。App Runner コンソールでは、ドメインのwwwサブドメインを含めることはできません。

> **Note**
>
> AWS App Runner は Route 53 プライベートホストゾーンの使用をサポートしていません。プライベートホストゾーンは、Amazon VPC トラフィックのドメイン名解決をカスタマイズします。プライベートホストゾーンの詳細については、Route 53 ドキュメントの「プライベートホストゾーンの使用」を参照してください。

カスタムドメインをサービスに関連付ける (リンクする)

カスタムドメインをサービスに関連付けるときは、CNAME レコードと DNS ターゲットレコードを DNS サーバーに追加する必要があります。以下のセクションでは、CNAME レコードと DNS ターゲットレコード、およびそれらの使用方法について説明します。

> **Note**
>
> DNS プロバイダーとして Amazon Route 53 を使用している場合、App Runner は、App Runner ウェブアプリケーションにリンクするために必要な証明書検証と DNS レコードを使用してカスタムドメインを自動的に設定します。これは、App Runner コンソールを使用してカスタムドメインをサービスにリンクするときに発生します。詳細については、以下のカスタムドメインの管理トピックを参照してください。

CNAME レコード

カスタムドメインをサービスに関連付けると、App Runner は証明書検証用の証明書検証レコードのセットを提供します。これらの証明書検証レコードをドメインネームシステム (DNS) サーバーに

追加する必要があります。App Runner が提供する証明書検証レコードを DNS サーバーに追加します。これにより、App Runner はドメインを所有または管理していることを検証できます。

> **Note**
>
> カスタムドメイン証明書を自動更新するには、DNS サーバーから証明書検証レコードを削除しないようにしてください。証明書の更新に関連する問題を解決する方法については、「」を参照してくださいthe section called “カスタムドメイン証明書の更新”。

App Runner は ACM を使用してドメインを検証します。DNS レコードで CAA レコードを使用している場合は、少なくとも 1 つの CAA レコードが を参照していることを確認してください`amazon.com`。それ以外の場合、ACM はドメインを検証してドメインを正常に作成できません。

CAA に関連するエラーが発生した場合の解決方法については、次のリンクを参照してください。

- 認証機関認可 (CAA) の問題
- ACM 証明書の発行または更新に関する CAA エラーを解決するにはどうすればよいですか？
- カスタムドメイン名

> **Note**
>
> DNS プロバイダーとして Amazon Route 53 を使用している場合、App Runner は、App Runner ウェブアプリケーションにリンクするために必要な証明書の検証と DNS レコードを使用してカスタムドメインを自動的に設定します。これは、App Runner コンソールを使用してカスタムドメインをサービスにリンクするときに発生します。詳細については、次のカスタムドメインの管理トピックを参照してください。

DNS ターゲットレコード

DNS ターゲットレコードを DNS サーバーに追加して、App Runner ドメインをターゲットにします。このオプションを選択した場合は、カスタムドメインに 1 つのレコードを追加し、wwwサブドメインに別のレコードを追加します。次に、App Runner コンソールでカスタムドメインのステータスがアクティブになるまで待ちます。これには通常数分かかりますが、最大 24 ~ 48 時間 (1 ~ 2 日) かかる場合があります。カスタムドメインが検証されると、App Runner はこのドメインからウェブアプリケーションへのトラフィックのルーティングを開始します。

> **Note**
>
> App Runner サービスとの互換性を高めるには、DNS プロバイダーとして Amazon Route 53 を使用することをお勧めします。Amazon Route 53 を使用してパブリック DNS レコードを管理しない場合は、DNS プロバイダーに連絡してレコードを追加する方法を確認してください。
>
> DNS プロバイダーとして Amazon Route 53 を使用している場合は、サブドメインに CNAME レコードまたはエイリアスレコードを追加できます。ルートドメインの場合は、エイリアスレコードを使用していることを確認してください。

Amazon Route 53 または別のプロバイダーからドメイン名を購入できます。Amazon Route 53 でドメイン名を購入するには、「Amazon Route 53 デベロッパーガイド」の「新しいドメインの登録」を参照してください。

Route 53 で DNS ターゲットを設定する方法については、Amazon Route 53 デベロッパーガイドの「リソースへのトラフィックのルーティング」を参照してください。

GoDaddy、Shopify、Hover などの他のレジストラで DNS ターゲットを設定する方法については、DNS ターゲットレコードの追加に関する特定のドキュメントを参照してください。

App Runner サービスに関連付けるドメインを指定する

App Runner サービスに関連付けるドメインは、次の方法で指定できます。

- ルートドメイン – DNS には固有の制限があるため、ルートドメイン名の CNAME レコードの作成がブロックされる可能性があります。たとえば、ドメイン名が の場合`example.com`、 のトラフィックを App Runner サービス`acme.example.com`にルーティングする CNAME レコードを作成できます。ただし、 のトラフィックを App Runner サービス`example.com`にルーティングする CNAME レコードを作成することはできません。ルートドメインを作成するには、エイリアスレコードを追加してください。

  エイリアスレコードは Route 53 に固有であり、CNAME レコードよりも以下の利点があります。

  - Route 53 では、ルートドメインまたはサブドメインのエイリアスレコードを作成できるため、柔軟性が向上します。たとえば、ドメイン名が の場合`example.com`、 `example.com`または のリクエストを App Runner サービス`acme.example.com`にルーティングするレコードを作成できます。
  - コスト効率が高くなります。これは、Route 53 がエイリアスレコードを使用してトラフィックをルーティングするリクエストに対して課金しないためです。

- サブドメイン – 例えば、 `login.example.com`または ですadmin.login.example.com。オプションで、同じオペレーションの一部としてwwwサブドメインを関連付けることもできます。サブドメインに CNAME レコードまたはエイリアスレコードを追加できます。
- ワイルドカード – 例: `*.example.com`。この場合、 `www`オプションを使用することはできません。ワイルドカードは、ルートドメインの直接サブドメインとしてのみ指定でき、それ自体でのみ指定できます。これらは有効な仕様ではありません: `login*.example.com`、`*.login.example.com`。このワイルドカード仕様は、すべての即時サブドメインを関連付け、ルートドメイン自体を関連付けません。ルートドメインは別のオペレーションで関連付ける必要があります。

より具体的なドメインの関連付けは、より具体的なドメインの関連付けよりも優先されます。たとえば、 は を`login.example.com`上書きします`*.example.com`。より具体的な関連付けの証明書と CNAME が使用されます。

次の例は、複数のカスタムドメインの関連付けを使用する方法を示しています。

1. サービスのホームページ`example.com`に関連付けます。を有効に`www`して を関連付けます`www.example.com`。
2. サービスのログインページ`login.example.com`に関連付けます。
3. カスタム「見つからない」ページ`*.example.com`に関連付けます。

カスタムドメインの関連付けを解除 (リンク解除)

App Runner サービスからカスタムドメインの関連付けを解除 (リンク解除) できます。ドメインのリンクを解除すると、App Runner はこのドメインからウェブアプリケーションへのトラフィックのルーティングを停止します。

> **Note**
>
> DNS サーバーから関連付けを解除したドメインのレコードを削除する必要があります。

App Runner は、ドメインの有効性を追跡する証明書を内部で作成します。これらの証明書は AWS Certificate Manager (ACM) に保存されます。App Runner は、ドメインがサービスから関連付け解除されてから、またはサービスが削除されてから 7 日間、これらの証明書を削除しません。

カスタムドメインの管理

次のいずれかの方法を使用して、App Runner サービスのカスタムドメインを管理します。

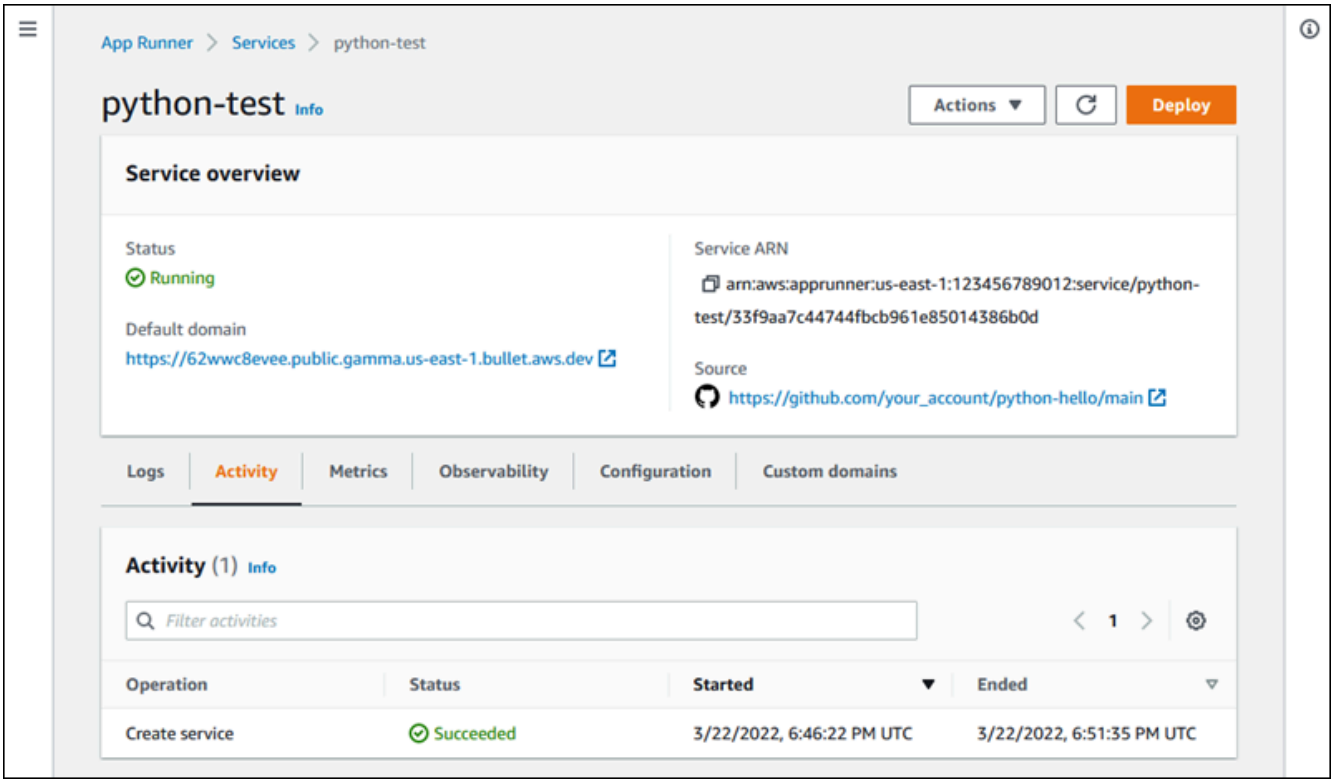
> **Note**
>
> App Runner サービスとの互換性を高めるには、DNS プロバイダーとして Amazon Route 53 を使用することをお勧めします。Amazon Route 53 を使用してパブリック DNS レコードを管理しない場合は、DNS プロバイダーに連絡してレコードを追加する方法を確認してください。
> DNS プロバイダーとして Amazon Route 53 を使用している場合は、サブドメインに CNAME レコードまたはエイリアスレコードを追加できます。ルートドメインの場合は、エイリアスレコードを使用していることを確認してください。

App Runner console

App Runner コンソールを使用してカスタムドメインを関連付け (リンク) するには

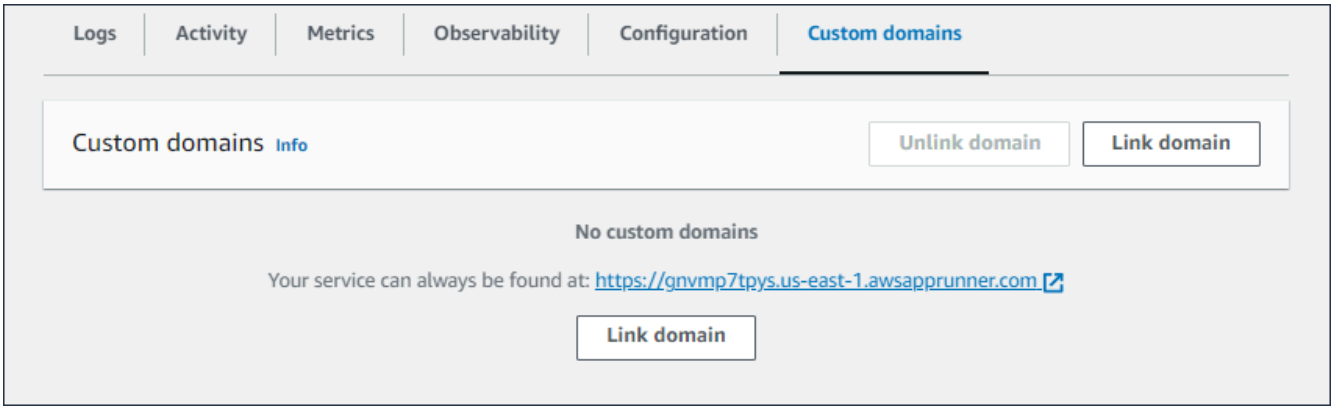
1. App Runner コンソールを開き、リージョンリストで を選択します AWS リージョン。
2. ナビゲーションペインで、サービスを選択し、App Runner サービスを選択します。

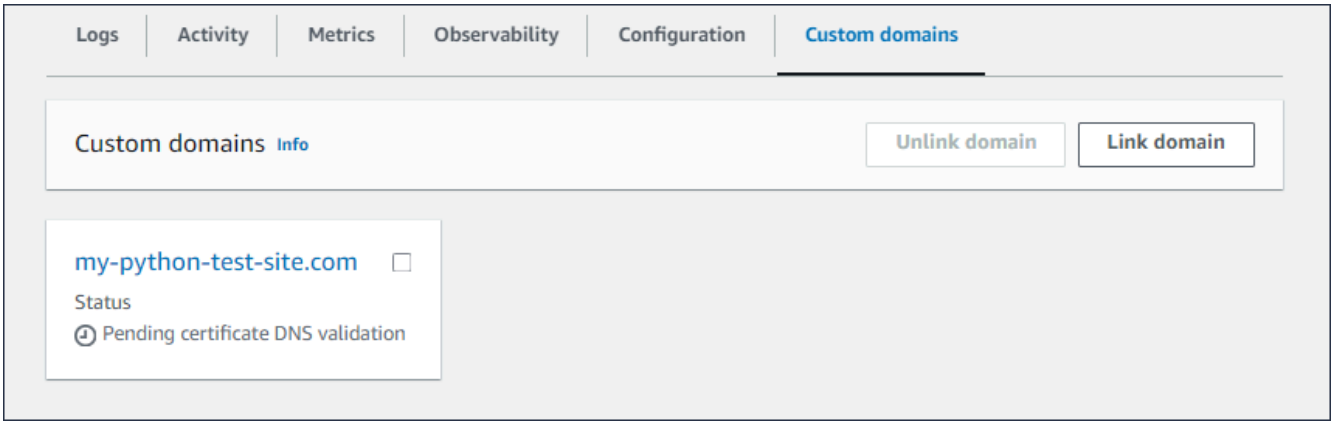
   コンソールには、サービスダッシュボードにサービスの概要が表示されます。



3. サービスダッシュボードページで、カスタムドメインタブを選択します。

コンソールには、サービスに関連付けられているカスタムドメイン、またはカスタムドメインなしが表示されます。

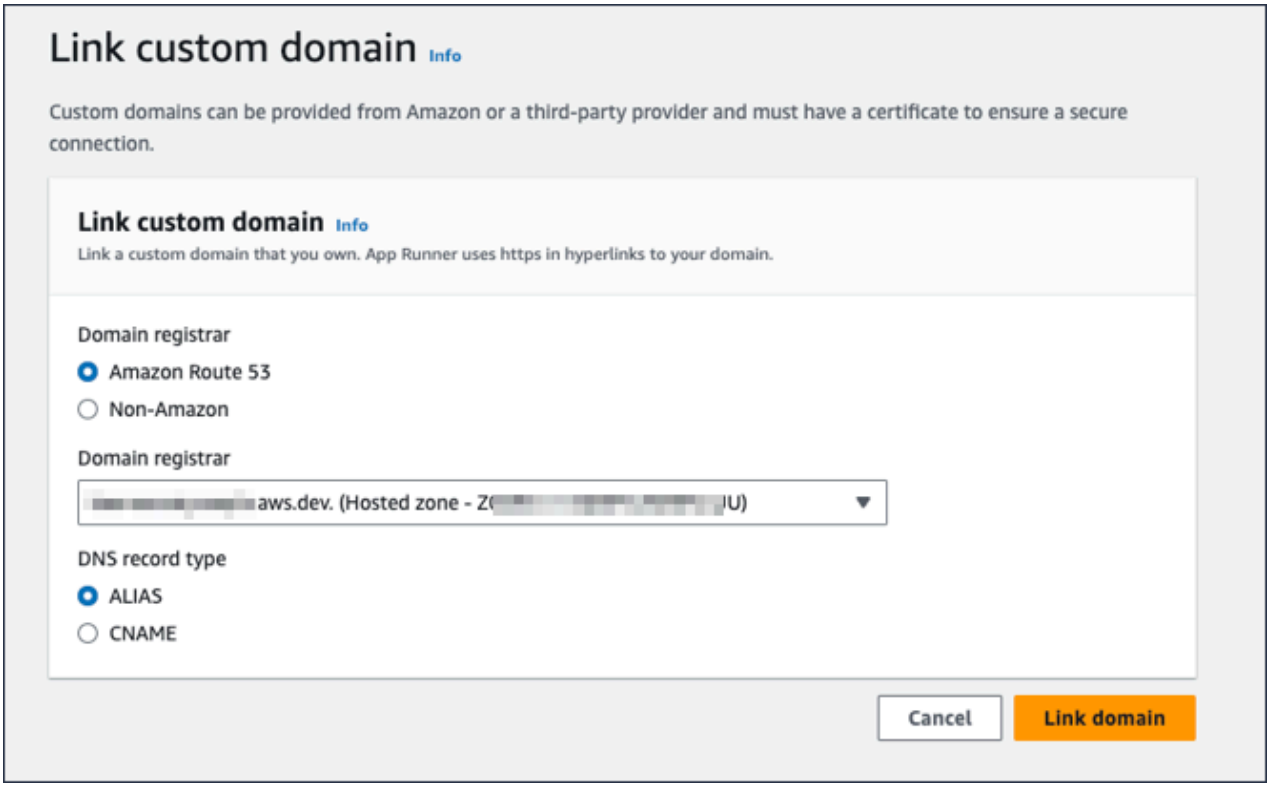




4. カスタムドメインタブで、ドメインのリンクを選択します。
5. カスタムドメインのリンクページが表示されます。
   - カスタムドメインが Amazon Route 53 に登録されている場合は、ドメインレジストラに Amazon Route 53 を選択します。
     a. ドロップダウンリストからドメイン名を選択します。このリストには、Route 53 ドメイン名とホストゾーン ID が表示されます。

     > **Note**
     > まず、他の App Runner リソースの管理に使用するのと同じ AWS アカウントから Amazon Route 53 サービスを使用して Route 53 ドメインを作成する必要があります。

     b. DNS レコードタイプを選択します。
     c. Link domain を選択します。

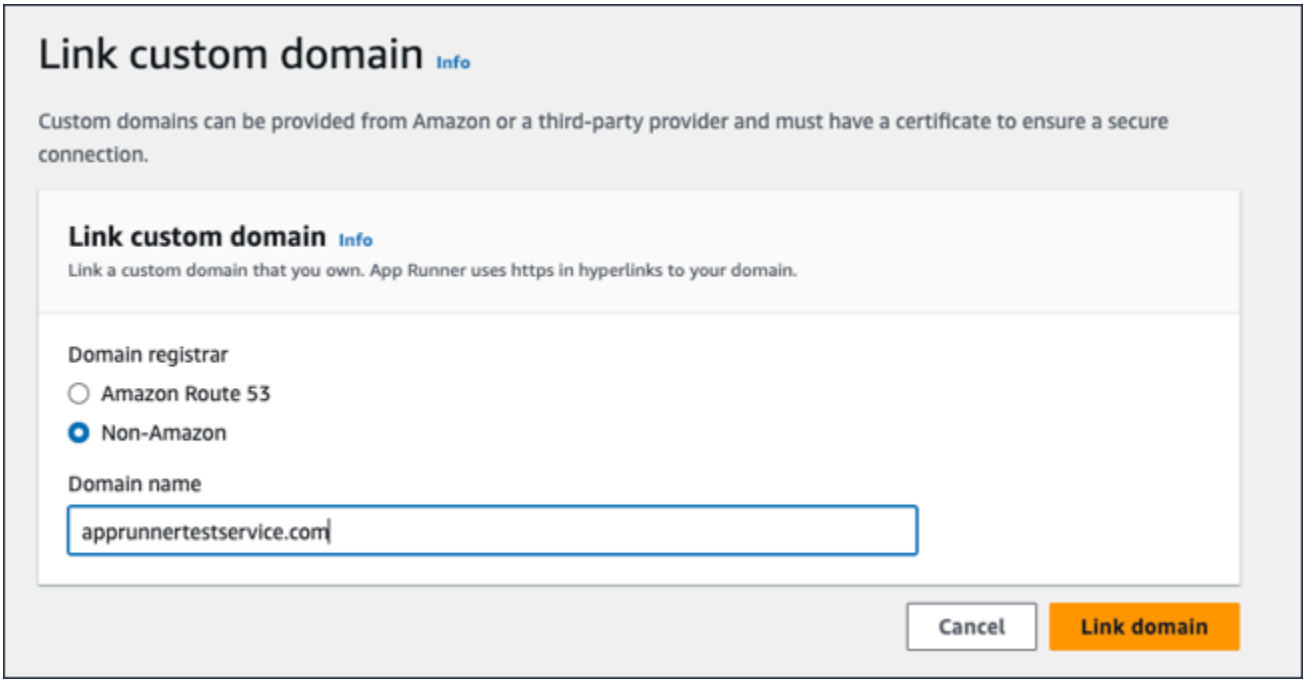


> **Note**
>
> App Runner で自動設定の試行が失敗したことを示すエラーメッセージが表示された場合は、DNS レコードを手動で設定して続行できます。この問題は、同じドメイン名が以前にサービスからリンク解除されていて、後でサービスを指す DNS プロバイダーレコードが削除されていない場合に発生する可能性があります。この場合、App Runner はこれらのレコードを自動的に上書きすることをブロックされます。DNS 設定を完了するには、この手順の残りのステップをスキップし、「」の手順に従いますAmazon Route 53 エイリアスレコードを設定する。

- カスタムドメインが別のドメインレジストラに登録されている場合は、ドメインレジストラに Amazon 以外の を選択します。

  a. ドメイン名を入力します。

  b. リンクドメインを選択します。



6. DNS の設定ページが表示されます。
   - Amazon Route 53 が DNS プロバイダーの場合、このステップはオプションです。

     この時点で、App Runner は、必要な証明書の検証と DNS レコードを使用して Route 53 ドメインを自動的に設定しました。

     > **Note**
     >
     > この同じドメイン名が以前にサービスからリンク解除され、後でサービスを指す DNS プロバイダーレコードが削除されなかった場合、App Runner が試行した自動設定が失敗した可能性があります。この問題を回避して DNS 関連付けを完了するには、DNS の設定ページのステップ (1) と (2) に進み、現在のターゲットレコードと証明書レコードを DNS プロバイダーにコピーします。

     - 証明書検証レコードと DNS ターゲットレコードをコピーし、DNS サーバーに追加します。App Runner は、ドメインを所有または管理していることを検証できます。

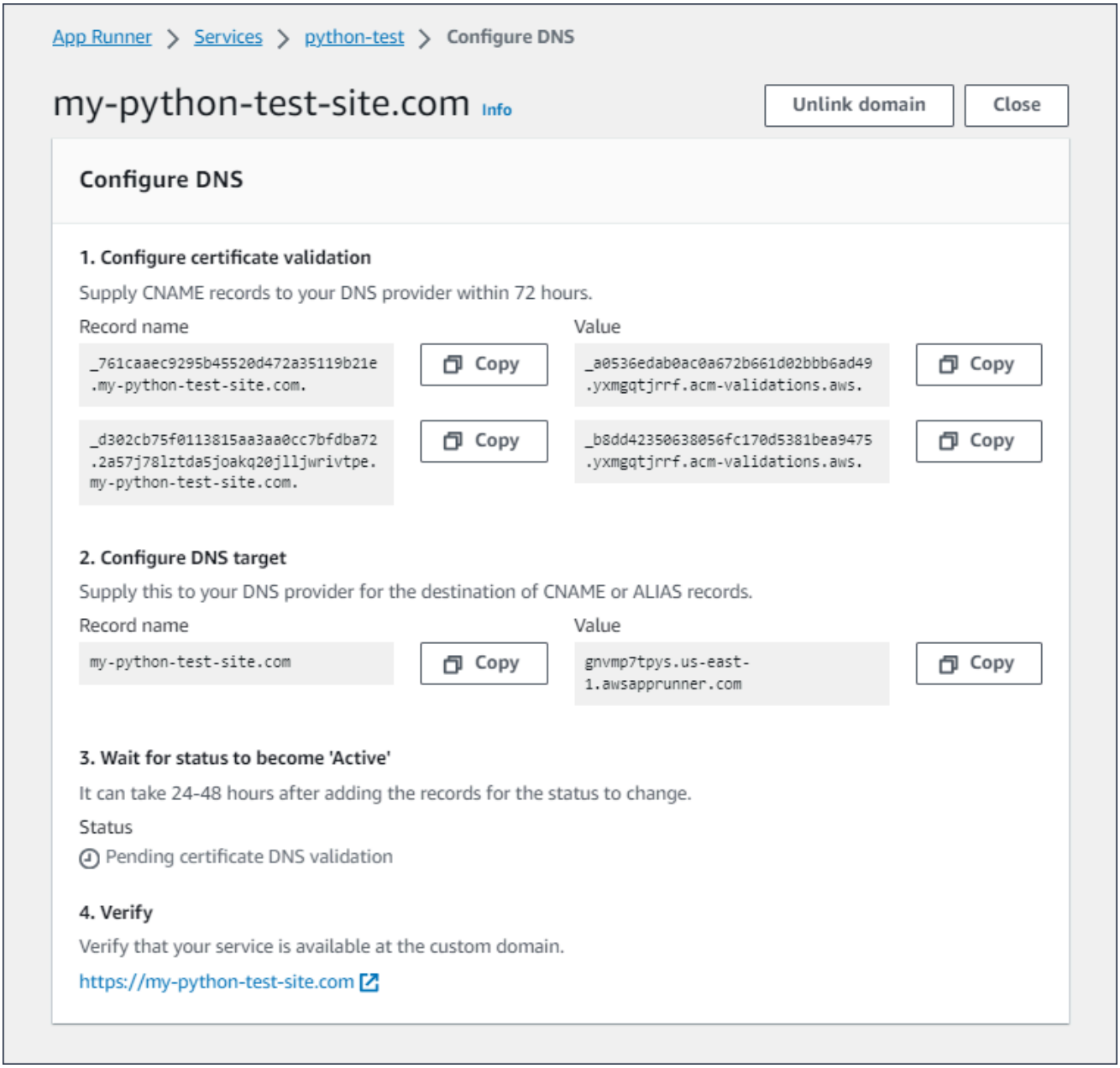
> **Note**
>
> カスタムドメイン証明書を自動更新するには、DNS サーバーから証明書検証レコードを削除しないようにしてください。

- 証明書検証の設定の詳細については、AWS Certificate Manager 「ユーザーガイド」の「DNS 検証」を参照してください。
- Amazon Route 53 エイリアスレコードで DNS ターゲットを設定する方法については、「」を参照してくださいthe section called “Amazon Route 53 エイリアスレコードを設定する”。

- Amazon Route 53 以外の DNS プロバイダーを使用している場合は、以下の手順に従います。
  - 証明書検証レコードと DNS ターゲットレコードをコピーし、DNS サーバーに追加します。App Runner は、ドメインを所有または管理していることを検証できます。

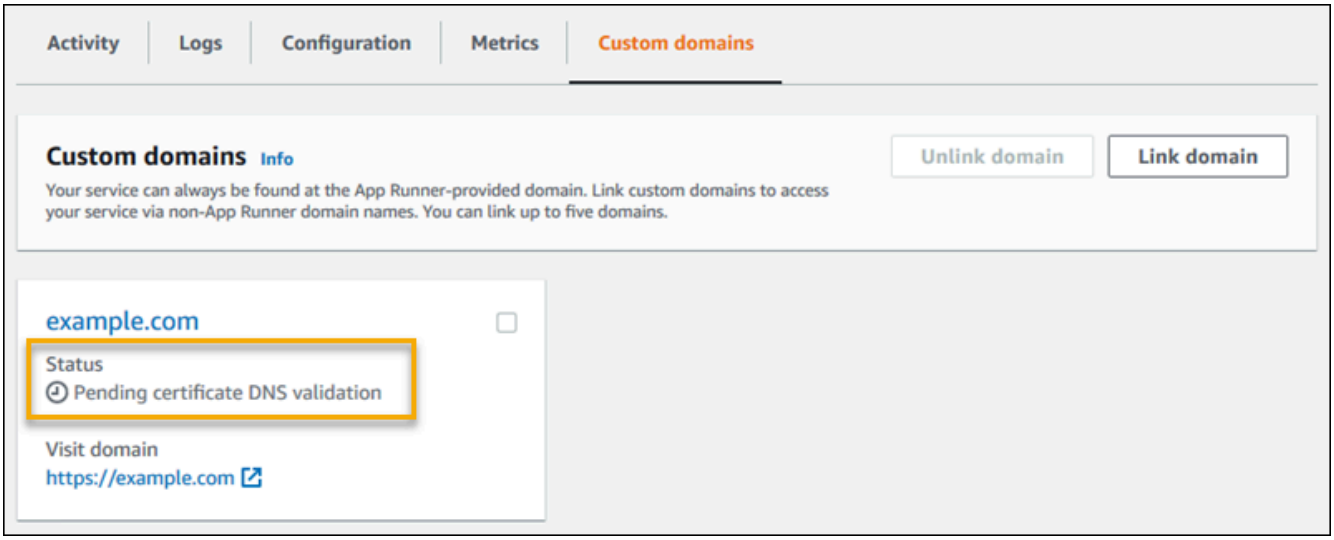
    > **Note**
    >
    > カスタムドメイン証明書を自動更新するには、DNS サーバーから証明書検証レコードを削除しないようにしてください。

    - 証明書検証の設定の詳細については、AWS Certificate Manager 「ユーザーガイド」の「DNS 検証」を参照してください。
    - GoDaddy、Shopify、Hover などの他のレジストラで DNS ターゲットを設定する方法については、DNS ターゲットの追加に関する特定のドキュメントを参照してください。

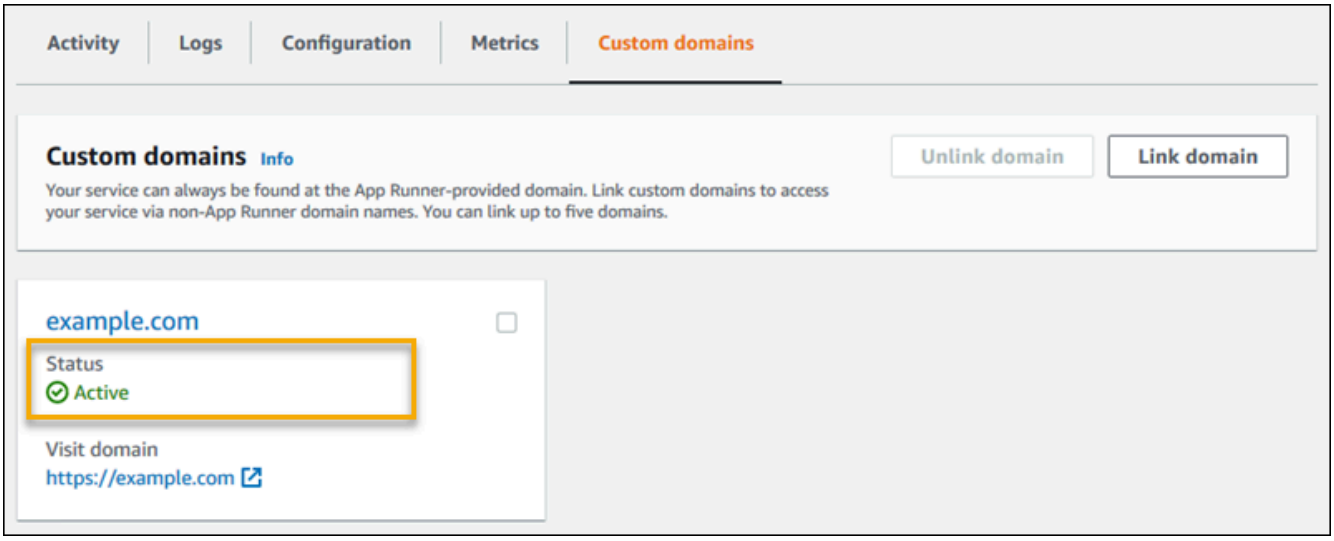


7. 閉じるを選択する

コンソールにダッシュボードが再度表示されます。カスタムドメインタブには、保留中の証明書 DNS 検証ステータスでリンクしたドメインを示す新しいタイルがあります。



8. ドメインのステータスがアクティブに変わったら、ドメインを参照してトラフィックをルーティングできることを確認します。



> **Note**
>
> カスタムドメインに関連するエラーをトラブルシューティングする方法については、「」を参照してくださいthe section called “カスタムドメイン名”。

App Runner コンソールを使用してカスタムドメインの関連付けを解除 (リンク解除) するには

1. カスタムドメインタブで、関連付けを解除するドメインのタイルを選択し、ドメインのリンク解除を選択します。

2. Unlink domain ダイアログで、Unlink domain を選択して アクションを確認します。

> **Note**
>
> DNS サーバーから関連付けを解除したドメインのレコードを削除する必要があります。

App Runner API or AWS CLI

App Runner API または を使用してカスタムドメインをサービスに関連付けるには AWS CLI、AssociateCustomDomain API アクションを呼び出します。呼び出しが成功すると、サービスに関連付けられているカスタムドメインを記述する CustomDomain オブジェクトが返されます。オブジェクトには`CREATING`ステータスが表示され、CertificateValidationRecord オブジェクトのリストが含まれます。この呼び出しは、DNS ターゲットの設定に使用できるターゲットエイリアスも返します。これらは、DNS に追加できるレコードです。

App Runner API または を使用してサービスからカスタムドメインの関連付けを解除するには AWS CLI、DisassociateCustomDomain API アクションを呼び出します。呼び出しが成功すると、サービスとの関連付けを解除するカスタムドメインを記述する CustomDomain オブジェクトが返されます。オブジェクトには`DELETING`ステータスが表示されます。

トピック

- ターゲット DNS の Amazon Route 53 エイリアスレコードを設定する

ターゲット DNS の Amazon Route 53 エイリアスレコードを設定する

> **Note**
>
> Amazon Route 53 が DNS プロバイダーである場合は、この手順に従う必要はありません。この場合、App Runner は、App Runner ウェブアプリケーションにリンクするために必要な証明書の検証と DNS レコードを使用して Route 53 ドメインを自動的に設定します。
> App Runner の自動設定の試行が失敗した場合は、次の手順に従って DNS 設定を完了します。同じドメイン名が以前にサービスからリンク解除され、後でサービスを指す DNS プロバイダーレコードが削除されなかった場合、App Runner はこれらのレコードを自動的に上

書きすることをブロックされます。この手順では、Route 53 DNS に手動でコピーする方法について説明します。

Amazon Route 53 を DNS プロバイダーとして使用して、トラフィックを App Runner サービスにルーティングできます。可用性が高くスケーラブルなドメインネームシステム (DNS) ウェブサービスです。Amazon Route 53 レコードには、App Runner サービスへのトラフィックのルーティング方法を制御する設定が含まれています。CNAME レコードまたは ALIAS レコードのいずれかを作成します。CNAME レコードとエイリアスレコードの比較については、「Amazon Route 53 デベロッパーガイド」の「エイリアスレコードと非エイリアスレコードの選択」を参照してください。

> **Note**
>
> Amazon Route 53 は現在、2022 年 8 月 1 日以降に作成されたサービスのエイリアスレコードをサポートしています。

Amazon Route 53 console

Amazon Route 53 エイリアスレコードを設定するには

1. にサインイン AWS Management Console し、Route 53 コンソールを開きます。
2. ナビゲーションペインで [Hosted zones] を選択します。
3. App Runner サービスへのトラフィックのルーティングに使用するホストゾーンの名前を選択します。
4. [Create record (レコードを作成)] を選択します。
5. 次の値を指定します。
   - ルーティングポリシー: 該当するルーティングポリシーを選択します。詳細については、「ルーティングポリシーの選択」を参照してください。
   - レコード名: App Runner サービスへのトラフィックのルーティングに使用するドメイン名を入力します。デフォルト値はホストゾーンの名前です。たとえば、ホストゾーンの名前が `example.com`で、 `acme.example.com`を使用してトラフィックを環境にルーティングする場合は、 と入力します`acme`。
   - 値/ルートトラフィックの送信先: App Runner アプリケーションへのエイリアスを選択し、エンドポイントの送信元のリージョンを選択します。トラフィックをルーティングするアプリケーションのドメイン名を選択します。

- レコードタイプ: デフォルトの A – IPv4 アドレスを受け入れます。
- ターゲットの状態を評価する: デフォルト値の「はい」を受け入れます。

6. [レコードを作成] を選択します。

作成した Route 53 エイリアスレコードは、60 秒以内にすべての Route 53 サーバーに伝播されます。Route 53 サーバーにエイリアスレコードが伝播されると、作成したエイリアスレコードの名前を使用してトラフィックを App Runner サービスにルーティングできます。

DNS の変更が反映されるまでに時間がかかりすぎる場合のトラブルシューティング方法については、「DNS の変更が Route 53 とパブリックリゾルバーに反映されるまでに時間がかかるのはなぜですか？」を参照してください。

Amazon Route 53 API or AWS CLI

Amazon Route 53 API を使用して Amazon Route 53 エイリアスレコードを設定するには、または ChangeResourceRecordSets API アクションを AWS CLI 呼び出します。Route 53 のターゲットホストゾーン ID については、「サービスエンドポイント」を参照してください。

App Runner サービスの一時停止と再開

ウェブアプリケーションを一時的に無効にしてコードの実行を停止する必要がある場合は、 AWS App Runner サービスを一時停止できます。App Runner は、サービスのコンピューティング容量をゼロに削減します。

アプリケーションを再度実行する準備ができたら、App Runner サービスを再開できます。App Runner は、新しいコンピューティングキャパシティをプロビジョニングし、アプリケーションをデプロイして、アプリケーションを実行します。アプリケーションソースは再デプロイされず、ビルドは必要ありません。むしろ、App Runner は現在デプロイされているバージョンで再開されます。アプリケーションは App Runner ドメインを保持します。

> **Important**
>
> - サービスを一時停止すると、アプリケーションの状態は失われます。たとえば、コードが使用したエフェメラルストレージはすべて失われます。コードの場合、サービスの一時停止と再開は、新しいサービスへのデプロイと同等です。
> - コードの欠陥 (検出されたバグやセキュリティの問題など) が原因でサービスを一時停止した場合、サービスを再開する前に新しいバージョンをデプロイすることはできません。

したがって、サービスを実行したまま、代わりに最後の安定したアプリケーションバージョンにロールバックすることをお勧めします。

- サービスを再開すると、App Runner はサービスを一時停止する前に使用された最後のアプリケーションバージョンをデプロイします。サービスの一時停止以降に新しいソースバージョンを追加した場合、自動デプロイが選択されていても、App Runner はそれらのバージョンを自動的にデプロイしません。たとえば、イメージリポジトリに新しいイメージバージョンがあるか、コードリポジトリに新しいコミットがあるとします。これらのバージョンは、自動的にデプロイされません。

  新しいバージョンをデプロイするには、App Runner サービスを再開した後に、手動デプロイを実行するか、別のバージョンをソースリポジトリに追加します。

比較した一時停止と削除

App Runner サービスを一時停止して一時的に無効にします。コンピューティングリソースのみが終了し、保存されたデータ (アプリケーションバージョンのコンテナイメージなど) はそのまま残ります。サービスの再開は迅速です。アプリケーションは新しいコンピューティングリソースにデプロイする準備が整います。App Runner ドメインは同じままです。

App Runner サービスを削除して、完全に削除します。保存されたデータは削除されます。サービスを再作成する必要がある場合、App Runner はソースを再度フェッチし、コードリポジトリの場合はビルドする必要があります。ウェブアプリケーションは、新しい App Runner ドメインを取得します。

サービスが一時停止したとき

サービスを一時停止し、一時停止ステータスになると、API コールやコンソールオペレーションなど、アクションリクエストに異なる方法で応答します。サービスを一時停止しても、ランタイムに影響する方法でサービスの定義や設定を変更しない App Runner アクションを実行できます。つまり、実行中のサービスの動作、スケール、またはその他の特性がアクションによって変更された場合、一時停止したサービスでそのアクションを実行することはできません。

次のリストは、一時停止したサービスで実行できる API アクションと実行できない API アクションに関する情報を示しています。同等のコンソールオペレーションも同様に許可または拒否されます。

一時停止したサービスで実行できるアクション

- *List** および *Describe**アクション – 情報のみを読み取るアクション。
- *DeleteService* – サービスはいつでも削除できます。
- *TagResource*、 *UntagResource* – タグはサービスに関連付けられていますが、その定義の一部ではなく、ランタイムの動作には影響しません。

一時停止したサービスで実行できないアクション

- *StartDeployment* アクション (または コンソールを使用した手動デプロイ)
- *UpdateService* (または、変更のタグ付けを除くコンソールを使用した設定変更)
- *CreateCustomDomainAssociations*, *DeleteCustomDomainAssociations*
- *CreateConnection*, *DeleteConnection*

サービスの一時停止と再開

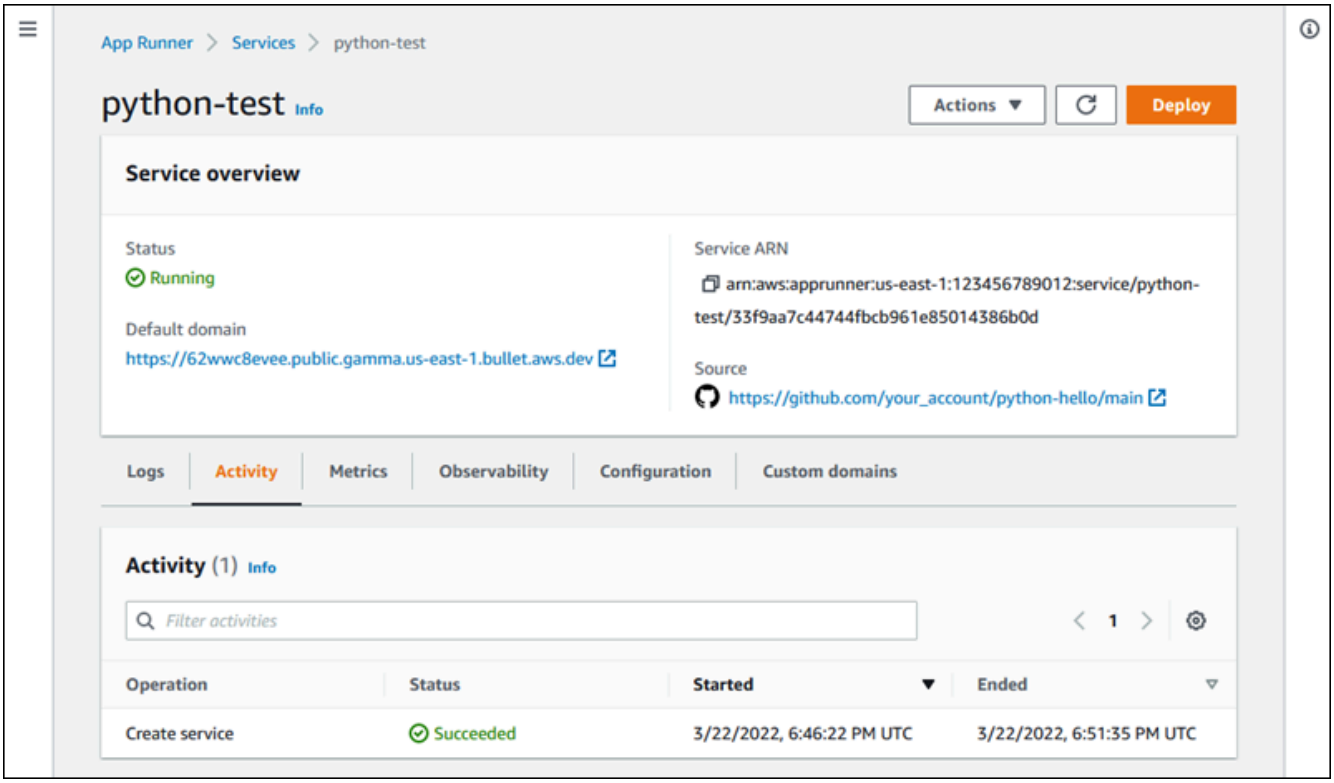
次のいずれかの方法を使用して、App Runner サービスを一時停止して再開します。

App Runner console

App Runner コンソールを使用してサービスを一時停止するには

1. App Runner コンソールを開き、リージョンリストで を選択します AWS リージョン。
2. ナビゲーションペインで、サービスを選択し、App Runner サービスを選択します。

   コンソールには、サービスダッシュボードにサービスの概要が表示されます。



3. アクションを選択し、一時停止を選択します。

   サービスダッシュボードページで、サービスのステータスが進行中のオペレーションに変わり、一時停止に変わります。これで、サービスは一時停止されます。

App Runner コンソールを使用してサービスを再開するには

1. アクションを選択し、再開を選択します。

   サービスダッシュボードページで、サービスのステータスが進行中のオペレーションに変わります。

2. サービスが再開されるまで待ちます。サービスダッシュボードページで、サービスのステータスが実行中に戻ります。

3. サービスの再開が成功したことを確認するには、サービスダッシュボードページで App Runner ドメイン値を選択します。これは、サービスのウェブサイトの URL です。ウェブアプリケーションが正しく実行されていることを確認します。

App Runner API or AWS CLI

App Runner API または を使用してサービスを一時停止するには AWS CLI、PauseService API アクションを呼び出します。呼び出しが を示すサービスオブジェクトで成功したレスポンスを返した場合`"Status": "OPERATION_IN_PROGRESS"`、App Runner はサービスの一時停止を開始します。

App Runner API または を使用してサービスを再開するには AWS CLI、ResumeService API アクションを呼び出します。呼び出しが を示す Service オブジェクトで成功したレスポンスを返した場合`"Status": "OPERATION_IN_PROGRESS"`、App Runner はサービスの再開を開始します。

App Runner サービスの削除

AWS App Runner サービスで実行されているウェブアプリケーションを終了する場合は、サービスを削除できます。サービスを削除すると、実行中のウェブサービスが停止し、基盤となるリソースが削除され、関連付けられたデータが削除されます。

次のいずれかの理由で App Runner サービスを削除できます。

- ウェブアプリケーションが不要になりました。例えば、廃止されたり、使用が終了した開発バージョンです。
- App Runner サービスクォータに達しました – 同じ で新しいサービスを作成し AWS リージョン 、アカウントに関連付けられたクォータに達しました。詳細については、「the section called “App Runner リソースクォータ”」を参照してください。
- セキュリティまたはプライバシーに関する考慮事項 – App Runner がサービスに保存するデータを削除する必要があります。

比較した一時停止と削除

App Runner サービスを一時停止して一時的に無効にします。コンピューティングリソースのみが終了し、保存されたデータ (アプリケーションバージョンのコンテナイメージなど) はそのまま残ります。サービスの再開は迅速で、アプリケーションを新しいコンピューティングリソースにデプロイする準備が整います。App Runner ドメインは同じままです。

App Runner サービスを削除して、完全に削除します。保存されたデータは削除されます。サービスを再作成する必要がある場合、App Runner はソースを再度取得し、コードリポジトリの場合はビルドする必要があります。ウェブアプリケーションは、新しい App Runner ドメインを取得します。

App Runner は何を削除しますか？

サービスを削除すると、App Runner は関連する項目の一部を削除し、他の項目は削除しません。次のリストに詳細を示します。

App Runner が削除する項目：

- コンテナイメージ – デプロイしたイメージまたは App Runner がソースコードから構築したイメージのコピー。App Runner AWS アカウント が所有する内部 を使用して Amazon Elastic Container Registry (Amazon ECR) に保存されます。
- サービス設定 – App Runner サービスに関連付けられている設定。App Runner AWS アカウント が所有する内部 を使用して Amazon DynamoDB に保存されます。

App Runner が削除しない項目：

- 接続 – サービスに関連付けられている接続がある可能性があります。App Runner 接続は、複数の App Runner サービス間で共有できる別のリソースです。接続が不要になった場合は、明示的に削除できます。詳細については、「the section called “Connections”」を参照してください。
- カスタムドメイン証明書 – カスタムドメインを App Runner サービスにリンクすると、App Runner はドメインの有効性を追跡する証明書を内部で作成します。これらは AWS Certificate Manager (ACM) に保存されます。App Runner は、ドメインがサービスからリンク解除されてから、またはサービスが削除されてから 7 日間、証明書を削除しません。詳細については、「the section called “カスタムドメイン名”」を参照してください。

サービスを削除する

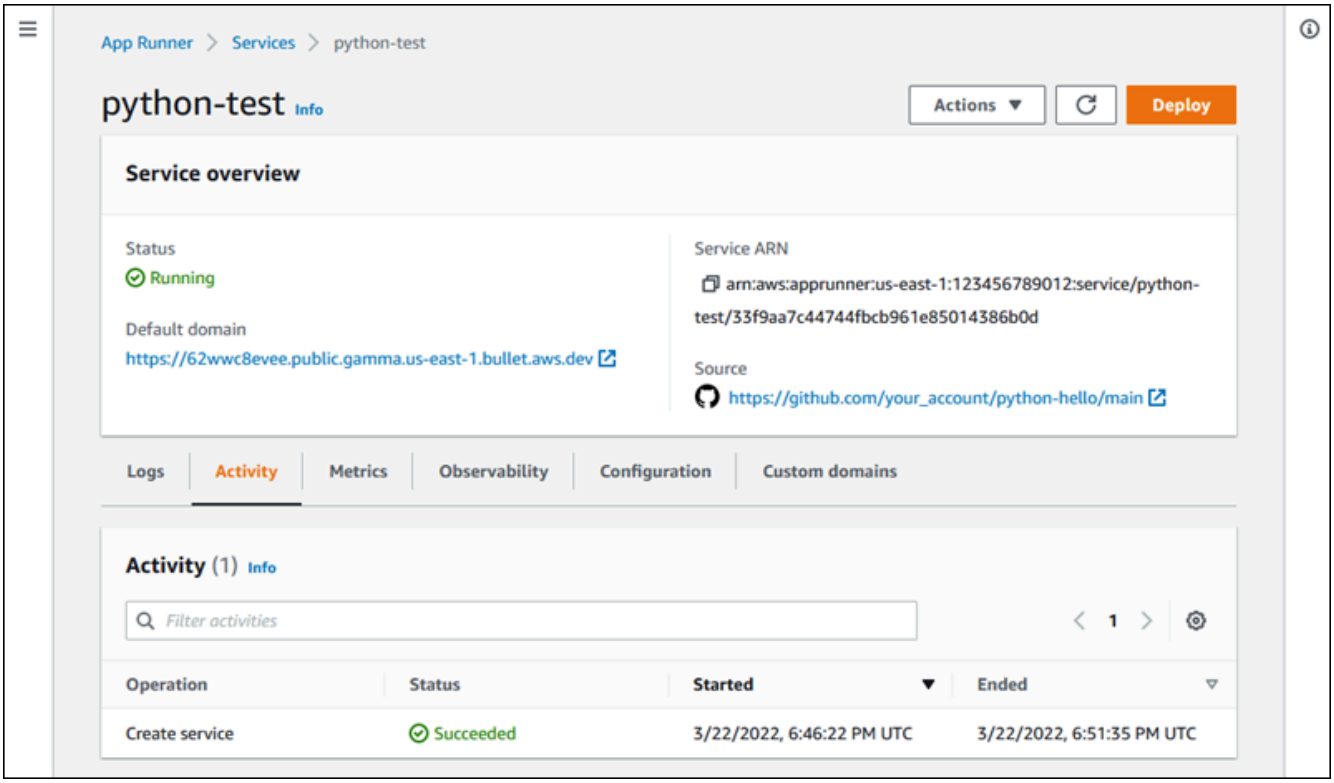
次のいずれかの方法を使用して App Runner サービスを削除します。

App Runner console

App Runner コンソールを使用してサービスを削除するには

1. App Runner コンソールを開き、リージョンリストで を選択します AWS リージョン。
2. ナビゲーションペインで、サービスを選択し、App Runner サービスを選択します。

   コンソールには、サービスダッシュボードにサービスの概要が表示されます。



3. [アクション] を選択し、[削除] を選択します。

   コンソールで サービスページに移動します。削除されるサービスに [進行中] とステータスが表示された後、サービスがリストから削除されます。これで、サービスが削除されます。

App Runner API or AWS CLI

App Runner API または を使用してサービスを削除するには AWS CLI、DeleteService API アクションを呼び出します。呼び出しが を示すサービスオブジェクトで成功したレスポンスを返した場合`"Status": "OPERATION_IN_PROGRESS"`、App Runner はサービスの削除を開始します。

環境変数の参照

App Runner を使用すると、サービスの作成時またはサービスの更新時に、シークレットと設定をサービス内の環境変数として参照できます。

プレーンテキストでは、タイムアウトや再試行回数などの機密性のない設定データをキーと値のペアとして参照できます。プレーンテキストで参照する設定データは暗号化されず、App Runner サービス設定とアプリケーションログで他のユーザーに表示されます。

> **Note**
>
> セキュリティ上の理由から、App Runner サービスのプレーンテキストの機密データは参照しないでください。

機密データを環境変数として参照する

App Runner は、機密データをサービス内の環境変数として安全に参照することをサポートしています。参照する機密データを AWS Secrets Managerまたは AWS Systems Manager Parameter Store に保存することを検討してください。次に、App Runner コンソールから、または API を呼び出して、サービスで環境変数として安全を参照できます。これにより、シークレットとパラメータの管理がアプリケーションコードとサービス設定から効果的に分離され、App Runner で実行されているアプリケーションの全体的なセキュリティが向上します。

> **Note**
>
> App Runner では、Secrets Manager と SSM パラメータストアを環境変数として参照しても料金は発生しません。ただし、Secrets Manager と SSM Parameter Store の使用には標準料金がかかります。
> 料金の詳細については、以下を参照してください。
>
> - AWS Secrets Manager の料金
> - AWS SSM パラメータストアの料金

機密データを環境変数として参照するプロセスを次に示します。

1. API キー、データベース認証情報、データベース接続パラメータ、アプリケーションバージョンなどの機密データをシークレットまたはパラメータとして AWS Secrets Manager または AWS Systems Manager パラメータストアに保存します。
2. App Runner が Secrets Manager と SSM パラメータストアに保存されているシークレットとパラメータにアクセスできるように、インスタンスロールの IAM ポリシーを更新します。詳細については、「アクセス許可」を参照してください。
3. 名前を割り当てて Amazon リソースネーム (ARN) を指定することで、シークレットとパラメータを環境変数として安全に参照します。サービスの作成時またはサービスの設定の更新時に、環境変数を追加できます。次のいずれかのオプションを使用して、環境変数を追加できます。
   - App Runner コンソール
   - App Runner API
   - `apprunner.yaml` 設定ファイル

   > **Note**
   > App Runner サービスを作成または更新するときに、環境変数の名前`PORT`として を割り当てることはできません。これは App Runner サービスの予約済み環境変数です。

   シークレットとパラメータを参照する方法の詳細については、「環境変数の管理」を参照してください。

> **Note**
> App Runner はシークレットとパラメータ ARNs への参照のみを保存するため、機密データは App Runner サービス設定とアプリケーションログの他のユーザーには表示されません。

考慮事項

- AWS Secrets Manager または Parameter Store の AWS Systems Manager シークレットとパラメータにアクセスするための適切なアクセス許可でインスタンスロールを更新してください。詳細については、「アクセス許可」を参照してください。

- AWS Systems Manager Parameter Store が、起動または更新するサービス AWS アカウント と同じ にあることを確認します。現在、アカウント間で SSM パラメータストアのパラメータを参照することはできません。
- シークレットとパラメータ値がローテーションまたは変更されると、App Runner サービスでは自動的に更新されません。App Runner はデプロイ中にのみシークレットとパラメータをプルするため、App Runner サービスを再デプロイします。
- また、App Runner サービスの SDK を使用して AWS Secrets Manager と AWS Systems Manager Parameter Store を直接呼び出すこともできます。
- エラーを回避するには、それらを環境変数として参照するときに、次の点を確認してください。
  - シークレットの正しい ARN を指定します。
  - パラメータの正しい名前または ARN を指定します。

アクセス許可

AWS Secrets Manager または SSM パラメータストアに保存されているシークレットとパラメータの参照を有効にするには、インスタンスロールの IAM ポリシーに適切なアクセス許可を追加して、Secrets Manager と SSM パラメータストアにアクセスします。

> **Note**
>
> App Runner は、ユーザーのアクセス許可がないと、アカウントのリソースにアクセスできません。アクセス許可は、IAM ポリシーを更新することで付与します。

次のポリシーテンプレートを使用して、IAM コンソールでインスタンスロールを更新できます。これらのポリシーテンプレートは、特定の要件を満たすように変更できます。インスタンスロールの更新の詳細については、「IAM ユーザーガイド」の「ロールの変更」を参照してください。

> **Note**
>
> 環境変数を作成するときに、App Runner コンソールから次のテンプレートをコピーすることもできます。

次のテンプレートをインスタンスロールにコピーして、 からシークレットを参照するアクセス許可を追加しますAWS Secrets Manager。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "secretsmanager:GetSecretValue",
        "kms:Decrypt*"
      ],
      "Resource": [
        "arn:aws:secretsmanager:<region>:<aws_account_id>:secret:<secret_name>",
        "arn:aws:kms:<region>:<aws_account_id>:key/<key_id>"
      ]
    }
  ]
}
```

次のテンプレートをインスタンスロールにコピーして、Parameter Store AWS Systems Manager からパラメータを参照するアクセス許可を追加します。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ssm:GetParameters"
      ],
      "Resource": [
        "arn:aws:ssm:<region>:<aws_account_id>:parameter/<parameter_name>"
      ]
    }
  ]
}
```

環境変数の管理

次のいずれかの方法を使用して、App Runner サービスの環境変数を管理します。

- the section called “App Runner コンソール”
- the section called “App Runner API または AWS CLI”

App Runner コンソール

App Runner コンソールでサービスを作成または更新するときに、環境変数を追加できます。

環境変数の追加

環境変数を追加するには

1. App Runner コンソールを開き、リージョンリストで を選択します AWS リージョン。
2. サービスを作成または更新するかどうかに基づいて、次のいずれかのステップを実行します。
   - 新しいサービスを作成する場合は、App Runner サービスの作成を選択し、サービスの設定に移動します。
   - 既存のサービスを更新する場合は、更新するサービスを選択し、サービスの設定タブに移動します。
3. 「サービス設定」の「環境変数 - オプション」に移動します。
4. 要件に基づいて、次のいずれかのオプションを選択します。
   - 環境変数のソースからプレーンテキストを選択し、それぞれ環境変数名と環境変数値の下にキーと値のペアを入力します。

     > **Note**
     > 機密性の高いデータを参照する場合は、プレーンテキストを選択します。このデータは暗号化されず、App Runner サービス設定とアプリケーションログで他のユーザーに表示されます。

   - 環境変数ソースから Secrets Manager を選択して、 に格納されているシークレットをサービスの環境変数 AWS Secrets Manager として参照します。参照するシークレットの環境変数名と Amazon リソースネーム (ARN) を、それぞれ環境変数名と環境変数値で指定します。
   - 環境変数ソースから SSM パラメータストアを選択して、SSM パラメータストアに保存されているパラメータをサービスの環境変数として参照します。参照するパラメータの環境変数名と ARN をそれぞれ環境変数名と環境変数値で指定します。

> **Note**
>
> - App Runner サービスを作成または更新するときに、環境変数の名前PORTとして を割り当てることはできません。これは App Runner サービスの予約済み環境変数です。
> - SSM Parameter Store パラメータが起動するサービス AWS リージョン と同じ にある場合は、完全な Amazon リソースネーム (ARN) またはパラメータの名前を指定できます。パラメータが別のリージョンにある場合は、完全な ARN を指定する必要があります。
> - 参照するパラメータが、起動または更新するサービスと同じアカウントにあることを確認します。現在、アカウント間で SSM パラメータストアパラメータを参照することはできません。

5. 環境変数を追加 を選択して、別の環境変数を参照します。
6. IAM ポリシーテンプレートを展開して、 および SSM パラメータストアに提供されている IAM ポリシーテンプレートを表示 AWS Secrets Manager およびコピーします。必要なアクセス許可でインスタンスロールの IAM ポリシーをまだ更新していない場合にのみ、これを行う必要があります。詳細については、「アクセス許可」を参照してください。

環境変数の削除

環境変数を削除する前に、アプリケーションコードが同じ内容を反映するように更新されていることを確認してください。アプリケーションコードが更新されない場合、App Runner サービスが失敗する可能性があります。

環境変数を削除するには

1. App Runner コンソールを開き、リージョンリストで を選択します AWS リージョン。
2. 更新するサービスの設定タブに移動します。
3. 「サービス設定」の「環境変数 - オプション」に移動します。
4. 削除する環境変数の横にある削除を選択します。削除を確認するメッセージが表示されます。
5. [削除] を選択します。

App Runner API または AWS CLI

Secrets Manager と SSM パラメータストアに保存されている機密データは、サービスに環境変数として追加することで参照できます。

> **Note**
>
> App Runner が Secrets Manager と SSM パラメータストアに保存されているシークレットとパラメータにアクセスできるように、インスタンスロールの IAM ポリシーを更新します。詳細については、「アクセス許可」を参照してください。

シークレットと設定を環境変数として参照するには

1. Secrets Manager または SSM パラメータストアでシークレットまたは設定を作成します。

   次の例は、SSM パラメータストアを使用してシークレットとパラメータを作成する方法を示しています。

   Example シークレットの作成 - リクエスト

   次の例は、データベース認証情報を表すシークレットを作成する方法を示しています。

   ```
   aws secretsmanager create-secret \
   –name DevRdsCredentials \
   –description "Rds credentials for development account." \
   –secret-string "{\"user\":\"diegor\",\"password\":\"EXAMPLE-PASSWORD\"}"
   ```

   Example シークレットの作成 - レスポンス

   ```
   arn:aws:secretsmanager:<region>:<aws_account_id>:secret:DevRdsCredentials
   ```

   Example 設定の作成 - リクエスト

   次の例は、RDS 接続文字列を表すパラメータを作成する方法を示しています。

   ```
   aws systemsmanager put-parameter \
   –name DevRdsConnectionString \
   –value "mysql2://dev-mysqlcluster-rds.com:3306/diegor" \
   –type "String" \
   ```

```
—description "Rds connection string for development account."
```

Example 設定の作成 - レスポンス

```
arn:aws:ssm:<region>:<aws_account_id>:parameter/DevRdsConnectionString
```

2. 環境変数として追加して、Secrets Manager と SSM パラメータストアに保存されているシークレットと設定を参照します。App Runner サービスを作成または更新するときに、環境変数を追加できます。

   次の例は、コードベースおよびイメージベースの App Runner サービスでシークレットと設定を環境変数として参照する方法を示しています。

   Example イメージベースの App Runner サービス用の Input.json ファイル

```
{
  "ServiceName": "example-secrets",
  "SourceConfiguration": {
    "ImageRepository": {
      "ImageIdentifier": "<image-identifier>",
      "ImageConfiguration": {
        "Port": "<port>",
        "RuntimeEnvironmentSecrets": {

 "Credential1":"arn:aws:secretsmanager:<region>:<aws_account_id>:secret:XXXXXXXXXXXX",
          "Credential2":"arn:aws:ssm:<region>:<aws_account_id>:parameter/
<parameter-name>"
        }
      },
      "ImageRepositoryType": "ECR_PUBLIC"
    }
  },
  "InstanceConfiguration": {
    "Cpu": "1 vCPU",
    "Memory": "3 GB",
    "InstanceRoleArn": "<instance-role-arn>"
  }
}
```

   Example イメージベースの App Runner サービス – リクエスト

```
aws apprunner create-service \
```

```
--cli-input-json file://input.json
```

Example イメージベースの App Runner サービス – レスポンス

```
{
...
      "ImageRepository": {
         "ImageIdentifier":"<image-identifier>",
         "ImageConfiguration":{
            "Port": "<port>",
            "RuntimeEnvironmentSecrets":{
               "Credential1":
 "arn:aws:secretsmanager:<region>:<aws_account_id>:secret:XXXXXXXXXXXX",
               "Credential2": "arn:aws:ssm:<region>:<aws_account_id>:parameter/
<parameter-name>"
            },
            "ImageRepositoryType":"ECR"
      }
   },
   "InstanceConfiguration": {
        "CPU": "1 vCPU",
        "Memory": "3 GB",
        "InstanceRoleArn: "<instance-role-arn>"
   }
...
}
```

Example コードベースの App Runner サービス用の Input.json ファイル

```
{
  "ServiceName": "example-secrets",
  "SourceConfiguration": {
    "AuthenticationConfiguration": {
      "ConnectionArn": "arn:aws:apprunner:us-east-1:123456789012:connection/my-
github-connection/XXXXXXXXXX"
    },
    "AutoDeploymentsEnabled": false,
    "CodeRepository": {
      "RepositoryUrl": "<repository-url>",
      "SourceCodeVersion": {
        "Type": "BRANCH",
        "Value": "main"
```

```
      },
      "CodeConfiguration": {
        "ConfigurationSource": "API",
        "CodeConfigurationValues": {
          "Runtime": "<runtime>",
          "BuildCommand": "<build-command>",
          "StartCommand": "<start-command>",
          "Port": "<port>",
          "RuntimeEnvironmentSecrets": {

 "Credential1":"arn:aws:secretsmanager:<region>:<aws_account_id>:secret:XXXXXXXXXXXX",
            "Credential2":"arn:aws:ssm:<region>:<aws_account_id>:parameter/
<parameter-name>"
          }
        }
      }
    }
  },
  "InstanceConfiguration": {
    "Cpu": "1 vCPU",
    "Memory": "3 GB",
    "InstanceRoleArn": "<instance-role-arn>"
  }
}
```

Example コードベースの App Runner サービス – リクエスト

```
aws apprunner create-service \
--cli-input-json file://input.json
```

Example コードベースの App Runner サービス – レスポンス

```
{
...
   "SourceConfiguration":{
      "CodeRepository":{
         "RepositoryUrl":"<repository-url>",
         "SourceCodeVersion":{
            "Type":"Branch",
            "Value":"main"
         },
         "CodeConfiguration":{
```

```
            "ConfigurationSource":"API",
            "CodeConfigurationValues":{
               "Runtime":"<runtime>",
               "BuildCommand":"<build-command>",
               "StartCommand":"<start-command>",
               "Port":"<port>",
               "RuntimeEnvironmentSecrets":{
                  "Credential1" :
 "arn:aws:secretsmanager:<region>:<aws_account_id>:secret:XXXXXXXX",
                  "Credential2" : "arn:aws:ssm:<region>:<aws_account_id>:parameter/
<parameter-name>"
               }
            }
         }
      },
      "InstanceConfiguration": {
        "CPU": "1 vCPU",
        "Memory": "3 GB",
        "InstanceRoleArn: "<instance-role-arn>"
   }
...
}
```

3. 追加されたシークレットを反映するようにapprunner.yamlモデルが更新されます。

   更新されたapprunner.yamlモデルの例を次に示します。

   Example **apprunner.yaml**

```
version: 1.0
runtime: python3
build:
  commands:
    build:
      - python -m pip install flask
run:
  command: python app.py
  network:
    port: 8080
  env:
    - name: MY_VAR_EXAMPLE
      value: "example"
  secrets:
    - name: my-secret
```

```
      value-from:
 "arn:aws:secretsmanager:<region>:<aws_account_id>:secret:XXXXXXXXXXXX"
    - name: my-parameter
      value-from: "arn:aws:ssm:<region>:<aws_account_id>:parameter/<parameter-
name>"
    - name: my-parameter-only-name
      value-from: "parameter-name"
```

App Runner を使用したネットワーク

この章では、 AWS App Runner サービスのネットワーク設定について説明します。

この章では、以下について説明します。

- プライベートエンドポイントとパブリックエンドポイントの受信トラフィックを設定する方法。詳細については、「受信トラフィックのネットワーク設定のセットアップ」を参照してください。
- Amazon VPC で実行されている他のアプリケーションにアクセスするように送信トラフィックを設定する方法。詳細については、「送信トラフィックの VPC アクセスの有効化」を参照してください。

> **Note**
>
> App Runner は現在、パブリック受信トラフィックに対してのみデュアルスタック (IPv4 および IPv6) アドレスタイプをサポートしています。送信トラフィックとプライベート受信トラフィックでは、IPv4 のみがサポートされます。

トピック

- 用語
- 受信トラフィックのネットワーク設定をセットアップする
- 送信トラフィックの VPC アクセスの有効化

用語

ニーズに合わせてネットワークトラフィックをカスタマイズする方法を理解するために、この章で使用されている以下の用語を理解しましょう。

一般的な用語

Amazon Virtual Private Cloud (VPC) に関連付けるために必要なことを知るために、次の用語を理解しましょう。

- VPC: Amazon VPC は、リソースの配置、接続、セキュリティなど、仮想ネットワーク環境を完全に制御できる論理的に分離された仮想ネットワークです。これは、独自のデータセンターで運用する従来のネットワークによく似た仮想ネットワークです。
- VPC インターフェイスエンドポイント: AWS PrivateLink リソースである VPC インターフェイスエンドポイントは、VPC をエンドポイントサービスに接続します。VPC インターフェイスエンドポイントを作成して、Network Load Balancer を使用してトラフィックを分散するエンドポイントサービスにトラフィックを送信します。エンドポイントサービス宛てのトラフィックは DNS を使用して解決されます。
- リージョン: 各リージョンは、App Runner サービスをホストできる個別の地理的エリアです。
- アベイラビリティーゾーン: アベイラビリティーゾーンは、 AWS リージョン内の独立した場所です。これは、冗長電源、ネットワーク、および接続を備えた 1 つ以上の個別のデータセンターです。アベイラビリティーゾーンは、本番環境アプリケーションの可用性、耐障害性、およびスケーラビリティを向上させるために役立ちます。
- サブネット: サブネットは VPC 内の IP アドレスの範囲です。サブネットは、1 つのアベイラビリティーゾーンに存在する必要があります。指定されたサブネットで AWS リソースを起動できます。インターネットに接続する必要があるリソースにはパブリックサブネットを、インターネットに接続しないリソースにはプライベートサブネットを使用してください。
- セキュリティグループ: セキュリティグループは、関連付けられているリソースに到達および送信できるトラフィックを制御します。セキュリティグループは、各サブネットの AWS リソースを保護するためのセキュリティレイヤーを追加し、ネットワークトラフィックをより詳細に制御できるようにします。VPC を作成すると、デフォルトのセキュリティグループが使用されます。VPC ごとに追加のセキュリティグループを作成できます。セキュリティグループは、それが作成された VPC 内のリソースにのみ関連付けることができます。
- デュアルスタック: デュアルスタックは、IPv4 エンドポイントと IPv6 エンドポイントの両方からのネットワークトラフィックをサポートするアドレスタイプです。

送信トラフィックの設定に固有の用語

VPC コネクタ

VPC Connector は、App Runner サービスがプライベート Amazon VPC で実行されるアプリケーションにアクセスできるようにする App Runner リソースです。

受信トラフィックの設定に固有の用語

Amazon VPC 内からのみサービスにプライベートにアクセスできるようにする方法については、次の用語を理解しましょう。

- VPC Ingress Connection: VPC Ingress Connection は、受信トラフィックの App Runner エンドポイントを提供する App Runner リソースです。App Runner コンソールで受信トラフィックのプライベートエンドポイントを選択すると、App Runner はバックグラウンドで VPC Ingress Connection リソースを割り当てます。VPC Ingress Connection リソースは、App Runner サービスを Amazon VPC の VPC インターフェイスエンドポイントに接続します。

> **Note**
>
> App Runner API を使用している場合、VPC Ingress Connection リソースは自動的に作成されません。

- プライベートエンドポイント: プライベートエンドポイントは、受信ネットワークトラフィックが Amazon VPC 内からのみアクセスできるように設定するために選択する App Runner コンソールオプションです。

受信トラフィックのネットワーク設定をセットアップする

プライベートエンドポイントまたはパブリックエンドポイントから受信トラフィックを受信するようにサービスを設定できます。

パブリックエンドポイントはデフォルト設定です。これにより、パブリックインターネットからの受信トラフィックに対してサービスが開きます。また、サービスのインターネットプロトコルバージョン 4 (IPv4) またはデュアルスタック (IPv4 および IPv6) アドレスタイプを柔軟に選択できます。

プライベートエンドポイントでは、Amazon VPC からのトラフィックのみが App Runner サービスにアクセスできます。これは、App Runner サービスの VPC インターフェイスエンドポイントである AWS PrivateLink リソースを設定することで実現されます。これにより、Amazon VPC と App Runner サービス間のプライベート接続が作成されます。

> **Note**
>
> App Runner は現在、パブリックエンドポイントでのみデュアルスタック (IPv4 および IPv6) アドレスタイプをサポートしています。プライベートエンドポイントでは、IPv4 のみがサポートされています。

以下は、受信トラフィックのネットワーク設定の設定の一環として説明するトピックです。

- Amazon VPC 内からのみサービスをプライベートに利用できるように受信トラフィックを設定する方法。詳細については、「受信トラフィックのプライベートエンドポイントの有効化」を参照してください。
- デュアルスタックアドレスタイプからインターネットトラフィックを受信するようにサービスを設定する方法。詳細については、「パブリック受信トラフィックのデュアルスタックの有効化」を参照してください。

ヘッダー

App Runner を使用すると、アプリケーションに入るトラフィックの元のソース IPv4 アドレスと IPv6 アドレスにアクセスできます。元の送信元 IP アドレスは、`X-Forwarded-For`リクエストヘッダーを割り当てることで保持されます。これにより、アプリケーションは必要に応じて元のソース IP アドレスを取得できます。

> **Note**
>
> サービスがプライベートエンドポイントを使用するように設定されている場合、`X-Forwarded-For`リクエストヘッダーを使用して元の送信元 IP アドレスにアクセスすることはできません。使用すると、false 値を取得します。

受信トラフィックのプライベートエンドポイントの有効化

デフォルトでは、 AWS App Runner サービスを作成すると、そのサービスはインターネット経由でアクセスできます。ただし、App Runner サービスをプライベートにして、Amazon Virtual Private Cloud (Amazon VPC) 内からのみアクセスできるようにすることもできます。

App Runner サービスプライベートを使用すると、受信トラフィックを完全に制御できるため、セキュリティレイヤーが追加されます。これは、内部 APIs、企業ウェブアプリケーション、またはよ

り高いレベルのプライバシーとセキュリティを必要とする開発中のアプリケーション、特定のコンプライアンス要件を満たす必要があるアプリケーションなど、さまざまなユースケースに役立ちます。

> **Note**
>
> App Runner アプリケーションにソース IP/CIDR 受信トラフィックコントロールルールが必要な場合は、WAF ウェブ ACLs の代わりにプライベートエンドポイントのセキュリティグループルールを使用する必要があります。これは、現在、リクエストソース IP データの WAF に関連付けられた App Runner プライベートサービスへの転送をサポートしていないためです。その結果、WAF ウェブ ACLsルールは、IP ベースのルールに準拠しません。ベストプラクティスを含むインフラストラクチャセキュリティおよびセキュリティグループの詳細については、「Amazon VPC ユーザーガイド」の「セキュリティグループを使用してネットワークトラフィックを制御し、AWS リソースへのトラフィックを制御する」を参照してください。 https://docs.aws.amazon.com/vpc/latest/userguide/vpc-security-groups.html

App Runner サービスがプライベートの場合は、Amazon VPC 内からサービスにアクセスできます。インターネットゲートウェイ、NAT デバイス、または VPN 接続は必要ありません。

> **Note**
>
> App Runner は現在、パブリック受信トラフィックに対してのみデュアルスタック (IPv4 および IPv6) アドレスタイプをサポートしています。送信トラフィックとプライベート受信トラフィックでは、IPv4 のみがサポートされます。

考慮事項

- App Runner の VPC インターフェイスエンドポイントを設定する前に、「 AWS PrivateLink ガイド」の「考慮事項」を確認してください。
- VPC エンドポイントポリシーは App Runner ではサポートされていません。デフォルトでは、VPC インターフェイスエンドポイントを介した App Runner へのフルアクセスが許可されます。または、セキュリティグループをエンドポイントネットワークインターフェイスに関連付けて、VPC インターフェイスエンドポイントを介して App Runner へのトラフィックを制御することもできます。

- App Runner アプリケーションにソース IP/CIDR 受信トラフィックコントロールルールが必要な場合は、WAF ウェブ ACLs の代わりにプライベートエンドポイントのセキュリティグループルールを使用する必要があります。これは、現在、リクエストソース IP データの WAF に関連付けられた App Runner プライベートサービスへの転送をサポートしていないためです。その結果、WAF ウェブ ACLsルールは、IP ベースのルールに準拠しません。
- プライベートエンドポイントを有効にすると、サービスは VPC からのみアクセスでき、インターネットからはアクセスできません。
- 可用性を高めるには、VPC インターフェイスエンドポイントの異なるアベイラビリティーゾーン全体で少なくとも 2 つのサブネットを選択することをお勧めします。サブネットを 1 つだけ使用することはお勧めしません。
- 同じ VPC インターフェイスエンドポイントを使用して、VPC 内の複数の App Runner サービスにアクセスできます。

このセクションで使用される用語の詳細については、「 用語」を参照してください。

アクセス許可

プライベートエンドポイントを有効にするために必要なアクセス許可のリストを次に示します。

- ec2:CreateTags
- ec2:CreateVpcEndpoint
- ec2:ModifyVpcEndpoint
- ec2:DeleteVpcEndpoints
- ec2:DescribeSubnets
- ec2:DescribeVpcEndpoints
- ec2:DescribeVpcs

VPC インターフェイスエンドポイント

VPC インターフェイスエンドポイントは、Amazon VPC をエンドポイントサービスに接続する AWS PrivateLinkリソースです。VPC インターフェイスエンドポイントを渡すことで、App Runner サービスにアクセスできるようにする Amazon VPC を指定できます。VPC インターフェイスエンドポイントを作成するには、以下を指定します。

- 接続を有効にする Amazon VPC。

- セキュリティグループを追加します。デフォルトでは、セキュリティグループは VPC インターフェイスエンドポイントに割り当てられます。カスタムセキュリティグループを関連付けて、受信ネットワークトラフィックをさらに制御できます。
- サブネットを追加します。可用性を高めるために、App Runner サービスにアクセスするアベイラビリティーゾーンごとに少なくとも 2 つのサブネットを選択することをお勧めします。ネットワークインターフェイスエンドポイントは、VPC インターフェイスエンドポイントに対して有効にする各サブネットに作成されます。これらは、App Runner 宛てのトラフィックのエントリポイントとして機能するリクエスタ管理のネットワークインターフェイスです。リクエスタマネージド型のネットワークインターフェイスは、 AWS のサービスがユーザーに代わって VPC 内に作成するネットワークインターフェイスです。
- API を使用している場合は、App Runner VPC インターフェイスエンドポイント を追加しますServicename。例えば、 などです

```
com.amazonaws.region.apprunner.requests
```

VPC インターフェイスエンドポイントは、次のいずれか AWS のサービスを使用して作成できます。

- App Runner コンソール。詳細については、「プライベートエンドポイントの管理」を参照してください。
- Amazon VPC コンソールまたは API、および AWS Command Line Interface （ AWS CLI ）。詳細については、「 AWS PrivateLink ガイド」の「 AWS のサービス からアクセス AWS PrivateLinkする」を参照してください。

> **Note**
>
> AWS PrivateLink 料金に基づいて、使用する VPC インターフェイスエンドポイントごとに課金されます。したがって、コスト効率を向上させるために、同じ VPC インターフェイスエンドポイントを使用して VPC 内の複数の App Runner サービスにアクセスできます。ただし、分離を改善するには、App Runner サービスごとに異なる VPC インターフェイスエンドポイントを関連付けることを検討してください。

VPC イングレス接続

VPC Ingress Connection は、受信トラフィックの App Runner エンドポイントを指定する App Runner リソースです。App Runner コンソールで受信トラフィックのプライベートエンドポイントを選択すると、App Runner はバックグラウンドで VPC Ingress Connection リソースを割り当てます。このオプションを選択すると、Amazon VPC からのトラフィックのみが App Runner サービスにアクセスできるようになります。VPC Ingress Connection リソースは、App Runner サービスを Amazon VPC の VPC インターフェイスエンドポイントに接続します。VPC Ingress Connection リソースは、 API オペレーションを使用して受信トラフィックのネットワーク設定を構成している場合にのみ作成できます。VPC Ingress Connection リソースを作成する方法の詳細については、 AWS App Runner API リファレンスのCreateVpcIngressConnection」を参照してください。

> **Note**
>
> App Runner の 1 つの VPC Ingress Connection リソースは、Amazon VPC の 1 つの VPC インターフェイスエンドポイントに接続できます。また、App Runner サービスごとに作成できる VPC Ingress Connection リソースは 1 つだけです。

プライベートエンドポイント

プライベートエンドポイントは、Amazon VPC からの受信トラフィックのみを受信する場合に選択できる App Runner コンソールオプションです。App Runner コンソールでプライベートエンドポイントオプションを選択すると、VPC インターフェイスエンドポイントを設定してサービスを VPC に接続するオプションが提供されます。バックグラウンドでは、App Runner は設定した VPC インターフェイスエンドポイントに VPC Ingress Connection リソースを割り当てます。

> **Note**
>
> プライベートエンドポイントでは、IPv4 ネットワークトラフィックのみがサポートされています。

概要

Amazon VPC からのトラフィックのみに App Runner サービスへのアクセスを許可して、サービスをプライベートにします。これを実現するには、App Runner または Amazon VPC を使用して、選択した Amazon VPC の VPC インターフェイスエンドポイントを作成します。App Runner コンソールで、受信トラフィックのプライベートエンドポイントを有効にすると、VPC インターフェイスエ

ンドポイントが作成されます。App Runner は、VPC Ingress Connection リソースを自動的に作成し、VPC インターフェイスエンドポイントと App Runner サービスに接続します。これにより、選択した VPC からのトラフィックのみが App Runner サービスにアクセスできるようにするプライベートサービス接続が作成されます。

プライベートエンドポイントの管理

次のいずれかの方法を使用して、受信トラフィックのプライベートエンドポイントを管理します。

- the section called “App Runner コンソール”
- the section called “App Runner API または AWS CLI”

> **Note**
>
> App Runner アプリケーションにソース IP/CIDR 受信トラフィックコントロールルールが必要な場合は、WAF ウェブ ACLs の代わりにプライベートエンドポイントのセキュリティグループルールを使用する必要があります。これは、現在、リクエストソース IP データの WAF に関連付けられた App Runner プライベートサービスへの転送をサポートしていないためです。その結果、WAF ウェブ ACLs に関連付けられている App Runner プライベートサービスのソース IP ルールは、IP ベースのルールに準拠しません。
> ベストプラクティスを含むインフラストラクチャセキュリティおよびセキュリティグループの詳細については、「Amazon VPC ユーザーガイド」の「セキュリティグループを使用してネットワークトラフィックを制御し、AWS リソースへのトラフィックを制御する」を参照してください。 https://docs.aws.amazon.com/vpc/latest/userguide/vpc-security-groups.html

App Runner コンソール

App Runner コンソールを使用してサービスを作成する場合、または後で設定を更新する場合は、受信トラフィックの設定を選択できます。

受信トラフィックを設定するには、次のいずれかを選択します。

- パブリックエンドポイント: インターネット経由ですべてのサービスからサービスにアクセスできるようにします。デフォルトでは、パブリックエンドポイントが選択されています。
- プライベートエンドポイント: Amazon VPC 内からのみ App Runner サービスにアクセスできるようにします。

> **Note**
>
> 現在、App Runner はパブリックエンドポイントに対してのみ IPv6 をサポートしています。IPv6 エンドポイントは、Amazon Virtual Private Cloud (Amazon VPC) でホストされている App Runner サービスではサポートされていません。デュアルスタックのパブリックエンドポイントを使用しているサービスをプライベートエンドポイントに更新すると、App Runner サービスはデフォルトで IPv4 エンドポイントからのトラフィックのみをサポートし、IPv6 エンドポイントからのトラフィックの受信に失敗します。

プライベートエンドポイントを有効にする

アクセスする Amazon VPC の VPC インターフェイスエンドポイントに関連付けることで、プライベートエンドポイントを有効にします。新しい VPC インターフェイスエンドポイントを作成するか、既存のエンドポイントを選択できます。

VPC インターフェイスエンドポイントを作成するには

1. App Runner コンソールを開き、リージョンリストで を選択します AWS リージョン。
2. 「サービスの設定」の「ネットワーク」セクションに移動します。
3. 受信ネットワークトラフィックにプライベートエンドポイントを選択します。VPC インターフェイスエンドポイントを使用して VCP に接続するオプションが開きます。
4. 新しいエンドポイントの作成 を選択します。新しい VPC インターフェイスエンドポイントの作成ダイアログボックスが開きます。
5. VPC インターフェイスエンドポイントの名前を入力します。
6. ドロップダウンリストから必要な VPC インターフェイスエンドポイントを選択します。
7. ドロップダウンリストからセキュリティグループを選択します。セキュリティグループを追加すると、VPC インターフェイスエンドポイントにセキュリティレイヤーが追加されます。2 つ以上のセキュリティグループを選択することをお勧めします。セキュリティグループを選択しない場合、App Runner は VPC インターフェイスエンドポイントにデフォルトのセキュリティグループを割り当てます。セキュリティグループルールが App Runner サービスと通信するリソースをブロックしていないことを確認します。セキュリティグループルールでは、App Runner サービスとやり取りするリソースを許可する必要があります。

> **Note**
>
> App Runner アプリケーションにソース IP/CIDR 受信トラフィックコントロールルールが必要な場合は、WAF ウェブ ACLs の代わりにプライベートエンドポイントのセキュリティグループルールを使用する必要があります。これは、現在、リクエストソース IP データの WAF に関連付けられた App Runner プライベートサービスへの転送をサポートしていないためです。その結果、WAF ウェブ ACLs に関連付けられている App Runner プライベートサービスのソース IP ルールは、IP ベースのルールに準拠しません。
> ベストプラクティスを含むインフラストラクチャセキュリティおよびセキュリティグループの詳細については、「Amazon VPC ユーザーガイド」の「セキュリティグループを使用してネットワークトラフィックを制御し、AWS リソースへのトラフィックを制御する」を参照してください。 https://docs.aws.amazon.com/vpc/latest/userguide/vpc-security-groups.html

8. ドロップダウンリストから必要なサブネットを選択します。App Runner サービスにアクセスするアベイラビリティーゾーンごとに少なくとも 2 つのサブネットを選択することをお勧めします。
9. (オプション) 新しいタグを追加を選択し、タグキーとタグ値を入力します。
10. [Create] (作成) を選択します。サービスの設定ページが開き、上部のバーに VPC インターフェイスエンドポイントが正常に作成されたことを示すメッセージが表示されます。

既存の VPC インターフェイスエンドポイントを選択するには

1. App Runner コンソールを開き、リージョンリストで を選択します AWS リージョン。
2. 「サービスの設定」の「ネットワーク」セクションに移動します。
3. 受信ネットワークトラフィックにプライベートエンドポイントを選択します。VPC インターフェイスエンドポイントを使用して VPC に接続するオプションが開きます。使用可能な VPC インターフェイスエンドポイントのリストが表示されます。
4. VPC インターフェイスエンドポイントにリストされている必要な VPC インターフェイスエンドポイントを選択します。
5. 次へ を選択してサービスを作成します。App Runner はプライベートエンドポイントを有効にします。

> **Note**
>
> サービスを作成したら、必要に応じて VPC インターフェイスエンドポイントに関連付けられたセキュリティグループとサブネットを編集できます。

プライベートエンドポイントの詳細を確認するには、サービスに移動し、設定タブのネットワークセクションを展開します。プライベートエンドポイントに関連付けられた VPC と VPC インターフェイスエンドポイントの詳細が表示されます。

VPC インターフェイスエンドポイントを更新する

App Runner サービスを作成したら、プライベートエンドポイントに関連付けられた VPC インターフェイスエンドポイントを編集できます。

> **Note**
>
> エンドポイント名と VPC フィールドを更新することはできません。

VPC インターフェイスエンドポイントを更新するには

1. App Runner コンソールを開き、リージョンリストで を選択します AWS リージョン。
2. サービスに移動し、左側のパネルでネットワーク設定を選択します。
3. 受信トラフィックを選択すると、それぞれのサービスに関連付けられている VPC インターフェイスエンドポイントが表示されます。
4. 編集する VPC インターフェイスエンドポイントを選択します。
5. [編集] を選択します。VPC インターフェイスエンドポイントを編集するダイアログボックスが開きます。
6. 必要なセキュリティグループとサブネットを選択し、更新をクリックします。VPC インターフェイスエンドポイントの詳細を示すページが開き、上部のバーに VPC インターフェイスエンドポイントが正常に更新されたことを示すメッセージが表示されます。

> **Note**
>
> App Runner アプリケーションにソース IP/CIDR 受信トラフィックコントロールルールが必要な場合は、WAF ウェブ ACLs の代わりにプライベートエンドポイントのセキュリティグループルールを使用する必要があります。これは、現在、リクエストソース IP データの WAF に関連付けられた App Runner プライベートサービスへの転送をサポートしていないためです。その結果、WAF ウェブ ACLs に関連付けられている App Runner プライベートサービスのソース IP ルールは、IP ベースのルールに準拠しません。
> ベストプラクティスを含むインフラストラクチャセキュリティおよびセキュリティグループの詳細については、「Amazon VPC ユーザーガイド」の「セキュリティグループを使用してネットワークトラフィックを制御し、AWS リソースへのトラフィックを制御する」を参照してください。 https://docs.aws.amazon.com/vpc/latest/userguide/vpc-security-groups.html

VPC インターフェイスエンドポイントを削除する

App Runner サービスにプライベートアクセスを許可しない場合は、受信トラフィックを Public に設定できます。をパブリックに変更すると、プライベートエンドポイントは削除されますが、VPC インターフェイスエンドポイントは削除されません。

VPC インターフェイスエンドポイントを削除するには

1. App Runner コンソールを開き、リージョンリストで を選択します AWS リージョン。
2. サービスに移動し、左側のパネルでネットワーク設定を選択します。
3. 受信トラフィックを選択すると、それぞれのサービスに関連付けられた VPC インターフェイスエンドポイントが表示されます。

> **Note**
>
> VPC インターフェイスエンドポイントを削除する前に、サービスを更新して、接続されているすべてのサービスから削除します。

4. [削除] を選択します。

VPC インターフェイスエンドポイントに接続されているサービスがある場合、VPC インターフェイスエンドポイントを削除できないというメッセージが表示されます。VPC インターフェイスエンドポイントに接続されているサービスがない場合は、削除を確認するメッセージが表示されます。

5. [削除] を選択します。着信トラフィックのネットワーク設定ページが開き、上部のバーに VPC インターフェイスエンドポイントが正常に削除されたというメッセージが表示されます。

App Runner API または AWS CLI

Amazon VPC 内からのみアクセスできるアプリケーションを App Runner にデプロイできます。

サービスをプライベートにするために必要なアクセス許可については、「」を参照してくださいthe section called “アクセス許可”。

> **Note**
>
> 現在、App Runner はパブリックエンドポイントに対してのみ IPv6 をサポートしています。IPv6 エンドポイントは、Amazon Virtual Private Cloud (Amazon VPC) でホストされている App Runner サービスではサポートされていません。デュアルスタックのパブリックエンドポイントを使用しているサービスをプライベートエンドポイントに更新すると、App Runner サービスはデフォルトで IPv4 エンドポイントからのトラフィックのみをサポートし、IPv6 エンドポイントからのトラフィックの受信に失敗します。

Amazon VPC へのプライベートサービス接続を作成するには

1. App Runner に接続する VPC インターフェイスエンドポイント、 AWS PrivateLink リソースを作成します。これを行うには、アプリケーションに関連付けるサブネットとセキュリティグループを指定します。VPC インターフェイスエンドポイントを作成する例を次に示します。

> **Note**
>
> App Runner アプリケーションにソース IP/CIDR 受信トラフィックコントロールルールが必要な場合は、WAF ウェブ ACLs の代わりにプライベートエンドポイントのセキュリティグループルールを使用する必要があります。これは、現在、リクエストソース IP データの WAF に関連付けられた App Runner プライベートサービスへの転送をサポートしていないためです。その結果、WAF ウェブ ACLs に関連付けられている App

Runner プライベートサービスのソース IP ルールは、IP ベースのルールに準拠しません。
ベストプラクティスを含むインフラストラクチャのセキュリティおよびセキュリティグループの詳細については、「Amazon VPC ユーザーガイド」の「セキュリティグループを使用してネットワークトラフィックを制御し、AWS リソースへのトラフィックを制御する」を参照してください。 https://docs.aws.amazon.com/vpc/latest/userguide/vpc-security-groups.html

Example

```
aws ec2 create-vpc-endpoint
 --vpc-endpoint-type: Interface
 --service-name: com.amazonaws.us-east-1.apprunner.requests
 --subnets: subnet1, subnet2
 --security-groups: sg1
```

2. CLI で CreateService または UpdateService App Runner API アクションを使用して、VPC インターフェイスエンドポイントを参照します。パブリックにアクセスできないようにサービスを設定します。`NetworkConfiguration` パラメータの `IngressConfiguration`メンバー`False`で を `IsPublicly Accessible`に設定します。VPC インターフェイスエンドポイントを参照する例を次に示します。

   Example

```
aws apprunner create-service
 --network-configuration: ingress-configuration=<ingress_configuration>
 --service-name: com.amazonaws.us-east-1.apprunner.requests
 --source-configuration: <source_configuration>
 # Ingress Configuration
 {
 "IsPubliclyAccessible": False
 }
```

3. `create-vpc-ingress-connection` API アクションを呼び出して App Runner の VPC Ingress Connection リソースを作成し、前のステップで作成した VPC インターフェイスエンドポイントに関連付けます。指定された VPC 内のサービスへのアクセスに使用されるドメイン名を返します。以下は、VPC Ingress Connection リソースを作成する例です。

Example リクエスト

```
aws apprunner create-vpc-ingress-connection
 --service-arn: <apprunner_service_arn>
 --ingress-vpc-configuration: {"VpcId":<vpc_id>, "VpceId": <vpce_id>}
 --vpc-ingress-connection-name: <vic_connection_name>
```

Example レスポンス

```
{
   "VpcIngressConnectionArn": <vpc_ingress_connection_arn>,
   "VpcIngressConnectionName": <vic_connection_name>,
   "ServiceArn": <apprunner_service_arn>,
   "Status": "PENDING_CREATION",
   "AccountId": <connection_owner_id>,
   "DomainName": <domain_name_associated_with_vpce>,
   "IngressVpcConfiguration": {"VpcId":<vpc_id>, "VpceId":<vpce_id>},
   "CreatedAt": <date_created>
}
```

VPC イングレス接続を更新する

VPC Ingress Connection リソースを更新できます。VPC イングレス接続を更新するには、次のいずれかの状態である必要があります。

- AVAILABLE
- 作成失敗
- FAILED_UPDATE

VPC Ingress Connection リソースを更新する例を次に示します。

Example リクエスト

```
aws apprunner update-vpc-ingress-connection
      --vpc-ingress-connection-arn: <vpc_ingress_connection_arn>
```

Example レスポンス

```
{
    "VpcIngressConnectionArn":  <vpc_ingress_connection_arn>,
    "VpcIngressConnectionName":  <vic_connection_name>,
    "ServiceArn":  <apprunner_service_arn>,
    "Status": "FAILED_UPDATE",
    "AccountId":  <connection_owner_id>,
    "DomainName":  <domain_name_associated_with_vpce>,
    "IngressVpcConfiguration": {"VpcId":<vpc_id>, "VpceId":<vpce_id>},
    "CreatedAt":  <date_created>
}
```

VPC イングレス接続を削除する

Amazon VPC へのプライベート接続が不要になった場合は、VPC Ingress Connection リソースを削除できます。

VPC イングレス接続を削除するには、次のいずれかの状態である必要があります。

- AVAILABLE
- 作成に失敗
- 更新に失敗
- 削除に失敗

VPC イングレス接続を削除する例を次に示します。

Example リクエスト

```
aws apprunner delete-vpc-ingress-connection
      --vpc-ingress-connection-arn: <vpc_ingress_connection_arn>
```

Example レスポンス

```
{
   "VpcIngressConnectionArn": <vpc_ingress_connection_arn>,
   "VpcIngressConnectionName": <vic_connection_name>,
   "ServiceArn": <apprunner_service_arn>,
   "Status": "PENDING_DELETION",
   "AccountId": <connection_owner_id>,
```

```
    "DomainName": <domain_name_associated_with_vpce>,
    "IngressVpcConfiguration": {"VpcId":<vpc_id>, "VpceId":<vpce_id>},
    "CreatedAt": <date_created>,
    "DeletedAt": <date_deleted>
}
```

次の App Runner API アクションを使用して、サービスのプライベートインバウンドトラフィックを管理します。

- CreateVpcIngressConnection – 新しい VPC Ingress Connection リソースを作成します。App Runner サービスを Amazon VPC エンドポイントに関連付ける場合、App Runner にはこのリソースが必要です。
- ListVpcIngressConnections – AWS アカウントに関連付けられている AWS App Runner VPC Ingress Connection エンドポイントのリストを返します。
- DescribeVpcIngressConnection – VPC Ingress Connection リソースの完全な AWS App Runner 説明を返します。
- UpdateVpcIngressConnection – AWS App Runner VPC Ingress Connection リソースを更新します。
- DeleteVpcIngressConnection – App Runner サービスに関連付けられている App Runner VPC Ingress Connection リソースを削除します。

App Runner API の使用の詳細については、「App Runner API リファレンスガイド」を参照してください。

パブリック着信トラフィックの IPv6 の有効化

サービスが IPv6 アドレス、または IPv4 アドレスと IPv6 アドレスの両方から受信ネットワークトラフィックを受信する場合は、パブリックエンドポイントのデュアルスタックアドレスタイプを選択します。新しいアプリケーションを作成するときは、「サービスの設定 > ネットワーク」セクションでこの設定を確認できます。App Runner コンソールまたは App Runner API を使用して IPv6 を有効にする方法の詳細については、「」を参照してくださいthe section called “パブリックエンドポイントのデュアルスタックを管理する”。

での IPv6 の採用の詳細については AWS、「 での IPv6 AWS」を参照してください。

App Runner は、パブリック App Runner サービスエンドポイントに対してのみデュアルスタックをサポートします。すべての App Runner プライベートサービスで、IPv4 のみがサポートされています。

> **Note**
>
> IP アドレスタイプをデュアルスタックに設定し、ネットワーク設定をパブリックエンドポイントからプライベートエンドポイントに変更すると、App Runner は自動的にアドレスタイプを IPv4 に変更します。これは、App Runner がパブリックエンドポイントに対してのみ IPv6 をサポートしているためです。

IPv4 と IPv6 の背景情報について説明します。

インターネット経由でネットワークトラフィックをルーティングするために一般的に使用される IPv4 ネットワークレイヤーは、32 ビットのアドレススキームを使用します。このアドレス空間は限られており、多数のネットワークデバイスで使い果たすことができます。このため、ネットワークアドレス変換 (NAT) は通常、1 つのパブリックネットワークアドレスを介して複数の IPv4 アドレスをルーティングするために使用されます。

インターネットプロトコルの最新バージョンである IPv6 は、IPv4 に基づいて構築され、128 ビットのアドレス指定スキームでアドレス空間を拡張します。IPv6 を使用すると、ほぼ無制限の数の接続されたデバイスでネットワークを構築できます。大量のネットワークアドレスがあるため、IPv6 では NAT は必要ありません。

IPv4 エンドポイントと IPv6 エンドポイントは相互に互換性がありません。IPv4 エンドポイントは受信 IPv6 トラフィックを受信できず、その逆も同様であるためです。デュアルスタックは、IPv4 と IPv6 の両方のネットワークトラフィックを同時にサポートできる便利なソリューションを提供します。

パブリック受信トラフィックのデュアルスタックの管理

次のいずれかの方法を使用して、パブリック着信トラフィックのデュアルスタックアドレスタイプを管理します。

- the section called “App Runner コンソール”
- the section called “App Runner API または AWS CLI”

App Runner コンソール

受信インターネットトラフィックのデュアルスタックアドレスタイプは、App Runner コンソールを使用してサービスを作成するとき、または後で設定を更新するときに選択できます。

デュアルスタックのアドレスタイプを有効にするには

1. サービスを作成または更新するときは、「サービスの設定」の「ネットワーク」セクションを展開します。
2. 受信ネットワークトラフィックにパブリックエンドポイントを選択します。パブリックエンドポイントの IP アドレスタイプオプションが開きます。
3. パブリックエンドポイントの IP アドレスタイプを展開して、次の IP アドレスタイプを表示します。

   - IPv4
   - デュアルスタック (IPv4 および IPv6)

   > **Note**
   > 選択を行うためにパブリックエンドポイントの IP アドレスタイプを展開しない場合、App Runner は IPv4 をデフォルト設定として割り当てます。

4. デュアルスタック (IPv4 および IPv6) を選択します。
5. サービスを作成する場合は、次へを選択し、次に作成とデプロイを選択します。それ以外の場合は、サービスを更新する場合は変更の保存を選択します。

   サービスがデプロイされると、アプリケーションは IPv4 エンドポイントと IPv6 エンドポイントの両方からネットワークトラフィックの受信を開始します。

> **Note**
> 現在、App Runner はパブリックエンドポイントに対してのみ IPv6 をサポートしています。IPv6 エンドポイントは、Amazon Virtual Private Cloud (Amazon VPC) でホストされている App Runner サービスではサポートされていません。デュアルスタックのパブリックエンドポイントを使用しているサービスをプライベートエンドポイントに更新すると、App Runner サービスはデフォルトで IPv4 エンドポイントからのトラフィックのみをサポートし、IPv6 エンドポイントからのトラフィックの受信に失敗します。

アドレスタイプを変更するには

1. 手順に従ってサービスを更新し、ネットワークに移動します。

2. 受信ネットワークトラフィックのパブリックエンドポイント IP アドレスタイプに移動し、必要なアドレスタイプを選択します。
3. [Save changes] (変更の保存) をクリックします。選択した内容でサービスが更新されます。

App Runner API または AWS CLI

CreateService または UpdateService App Runner API アクションを呼び出すときは、`NetworkConfiguration`パラメータ`IpAddressType`のメンバーを使用してアドレスタイプを指定します。指定できるサポートされている値は、 `IPv4`と ですDUAL_STACK。サービスが IPv4 および IPv6 エンドポイントからインターネットトラフィックを受信するDUAL_STACKかどうかを指定します。に値を指定しない場合`IpAddressType`、デフォルトで IPv4 が適用されます。

以下は、デュアルスタックを IP アドレスとしてサービスを作成する例です。この例では、`input.json`ファイルを呼び出します。

Example デュアルスタックをサポートするサービスの作成をリクエストする

```
aws apprunner create-service \
 --cli-input-json file://input.json
```

Example **`input.json`** の内容

```
{
  "ServiceName": "example-service",
  "SourceConfiguration": {
    "ImageRepository": {
      "ImageIdentifier": "public.ecr.aws/aws-containers/hello-app-runner:latest",
      "ImageConfiguration": {
        "Port": "8000"
      },
      "ImageRepositoryType": "ECR_PUBLIC"
    },
    "NetworkConfiguration": {
      "IpAddressType": "DUAL_STACK"
    }
  }
}
```

Example レスポンス

```
{
```

```
  "Service": {
    "ServiceName": "example-service",
    "ServiceId": "<service-id>",
    "ServiceArn": "arn:aws:apprunner:us-east-2:123456789012:service/example-
service/<service-id>",
    "ServiceUrl": "1234567890.us-east-2.awsapprunner.com",
    "CreatedAt": "2023-10-16T12:30:51.724000-04:00",
    "UpdatedAt": "2023-10-16T12:30:51.724000-04:00",
    "Status": "OPERATION_IN_PROGRESS",
    "SourceConfiguration": {
      "ImageRepository": {
        "ImageIdentifier": "public.ecr.aws/aws-containers/hello-app-runner:latest",
        "ImageConfiguration": {
          "Port": "8000"
        },
        "ImageRepositoryType": "ECR_PUBLIC"
      },
      "AutoDeploymentsEnabled": false
    },
    "InstanceConfiguration": {
      "Cpu": "1024",
      "Memory": "2048"
    },
    "HealthCheckConfiguration": {
      "Protocol": "TCP",
      "Path": "/",
      "Interval": 5,
      "Timeout": 2,
      "HealthyThreshold": 1,
      "UnhealthyThreshold": 5
    },
    "AutoScalingConfigurationSummary": {
      "AutoScalingConfigurationArn": "arn:aws:apprunner:us-
east-2:123456789012:autoscalingconfiguration/
DefaultConfiguration/1/00000000000000000000000000000001",
      "AutoScalingConfigurationName": "DefaultConfiguration",
      "AutoScalingConfigurationRevision": 1
    },
    "NetworkConfiguration": {
      "IpAddressType": "DUAL_STACK",
      "EgressConfiguration": {
        "EgressType": "DEFAULT"
      },
      "IngressConfiguration": {
```

```
        "IsPubliclyAccessible": true
      }
    }
  },
  "OperationId": "24bd100b1e111ae1a1f0e1115c4f11de"
}
```

> **Note**
>
> 現在、App Runner はパブリックエンドポイントに対してのみ IPv6 をサポートしています。IPv6 エンドポイントは、Amazon Virtual Private Cloud (Amazon VPC) でホストされている App Runner サービスではサポートされていません。デュアルスタックのパブリックエンドポイントを使用しているサービスをプライベートエンドポイントに更新すると、App Runner サービスはデフォルトで IPv4 エンドポイントからのトラフィックのみをサポートし、IPv6 エンドポイントからのトラフィックの受信に失敗します。

API パラメータの詳細については、NetworkConfiguration」を参照してください。

送信トラフィックの VPC アクセスの有効化

デフォルトでは、 AWS App Runner アプリケーションはパブリックエンドポイントにメッセージを送信できます。これには、独自のソリューション AWS のサービス、およびその他のパブリックウェブサイトまたはウェブサービスが含まれます。アプリケーションは、Amazon Virtual Private Cloud (Amazon VPC) から VPC で実行されるアプリケーションのパブリックエンドポイントにメッセージを送信することもできます。環境の起動時に VPC を設定しない場合、App Runner はパブリックであるデフォルトの VPC を使用します。

カスタム VPC で環境を起動して、送信トラフィックのネットワーク設定とセキュリティ設定をカスタマイズできます。 AWS App Runner サービスが Amazon Virtual Private Cloud (Amazon VPC) からプライベート VPC で実行されるアプリケーションにアクセスできるようにします。これを行うと、アプリケーションは に接続し、Amazon Virtual Private Cloud (Amazon VPC) でホストされている他のアプリケーションにメッセージを送信できます。例としては、Amazon RDS データベース、Amazon ElastiCache、およびプライベート VPC でホストされているその他のプライベートサービスがあります。

VPC コネクタ

VPC Connector と呼ばれる App Runner コンソールから VPC エンドポイントを作成することで、サービスを VPC に関連付けることができます。VPC コネクタを作成するには、VPC、1 つ以上のサブネット、およびオプションで 1 つ以上のセキュリティグループを指定します。VPC コネクタを設定したら、1 つ以上の App Runner サービスで使用できます。

1 回限りのレイテンシー

アウトバウンドトラフィック用にカスタム VPC コネクタを使用して App Runner サービスを設定すると、1 回限りの起動レイテンシーが 2~5 分になることがあります。スタートアッププロセスは、VPC Connector が他のリソースに接続する準備ができるまで待ってから、サービスステータスを実行中に設定します。サービスを最初に作成するときにカスタム VPC コネクタを使用して設定することも、後でサービスの更新を行って設定することもできます。

同じ VPC コネクタ設定を別のサービスに再利用しても、レイテンシーは発生しないことに注意してください。VPC コネクタの設定は、セキュリティグループとサブネットの組み合わせに基づいています。特定の VPC コネクタ設定では、レイテンシーは VPC Connector Hyperplane ENIs (Elastic Network Interface) の初回作成時に 1 回のみ発生します。

カスタム VPC コネクタと AWS Hyperplane の詳細

App Runner の VPC コネクタは、Network Load Balancer、NAT Gateway、AWS PrivateLink などの複数の AWS リソースの背後にある内部 Amazon ネットワークシステムである AWS Hyperplane に基づいています。 AWS Hyperplane テクノロジーは、高スループットと低レイテンシーの機能に加えて、より高いレベルの共有を提供します。Hyperplane ENI は、VPC コネクタを作成してサービスに関連付けると、サブネットに作成されます。VPC コネクタの設定はセキュリティグループとサブネットの組み合わせに基づいており、複数の App Runner サービスで同じ VPC コネクタを参照できます。その結果、基盤となる Hyperplane ENIs は App Runner サービス間で共有されます。この共有は、リクエストの負荷を処理するために必要なタスクの数をスケールアップしても実行可能であり、VPC 内の IP スペースをより効率的に使用できます。詳細については、AWS コンテナブログの「Deep Dive on AWS App Runner VPC Networking」を参照してください。

サブネット

各サブネットは特定のアベイラビリティーゾーンにあります。高可用性を実現するには、少なくとも 3 つのアベイラビリティーゾーンにまたがるサブネットを選択することをお勧めします。リージョンのアベイラビリティーゾーンが 3 つ未満の場合は、サポートされているすべてのアベイラビリティーゾーンでサブネットを選択することをお勧めします。

VPC のサブネットを選択するときは、パブリックサブネットではなくプライベートサブネットを選択するようにしてください。これは、VPC コネクタを作成すると、App Runner サービスが各サブネットに Hyperplane ENI を作成するためです。各 Hyperplane ENI にはプライベート IP アドレスのみが割り当てられ、AWSAppRunnerManaged キーのタグが付けられます。パブリックサブネットを選択すると、App Runner サービスの実行時にエラーが発生します。ただし、サービスがインターネットまたは他のパブリックサービスにアクセスする必要がある場合は AWS のサービス、「」を参照してくださいthe section called “サブネットを選択する際の考慮事項 ”。

サブネットを選択する際の考慮事項

- サービスを VPC に接続すると、アウトバウンドトラフィックはパブリックインターネットにアクセスできません。アプリケーションからのすべてのアウトバウンドトラフィックは、サービスが接続されている VPC を介して送信されます。VPC のすべてのネットワークルールは、アプリケーションのアウトバウンドトラフィックに適用されます。つまり、サービスはパブリックインターネットと AWS APIs にアクセスできません。アクセスするには、次のいずれかを実行します。
  - NAT ゲートウェイを介してサブネットをインターネットに接続します。
  - アクセス AWS のサービス する の VPC エンドポイントを設定します。サービスは、 を使用して Amazon VPC 内に留まります AWS PrivateLink。
- の一部のアベイラビリティーゾーンは、App Runner サービスで使用できるサブネットをサポート AWS リージョン していません。これらのアベイラビリティーゾーンでサブネットを選択すると、サービスの作成または更新に失敗します。このような状況では、App Runner はサポートされていないサブネットとアベイラビリティーゾーンを指す詳細なエラーメッセージを提供します。これが発生した場合は、サポートされていないサブネットをリクエストから削除してトラブルシューティングを行い、もう一度試してください。

セキュリティグループ

オプションで、指定したサブネット AWS で App Runner がアクセスするために使用するセキュリティグループを指定できます。セキュリティグループを指定しない場合、App Runner は VPC のデフォルトのセキュリティグループを使用します。デフォルトのセキュリティグループでは、すべてのアウトバウンドトラフィックを許可します。

セキュリティグループを追加すると、VCP コネクタにセキュリティレイヤーが追加され、ネットワークトラフィックをより詳細に制御できます。VPC コネクタは、アプリケーションからのアウトバウンド通信にのみ使用されます。アウトバウンドルールを使用して、目的の宛先エンドポイントへの通信を許可します。また、送信先リソースに関連付けられているセキュリティグループに適切な

インバウンドルールがあることを確認する必要があります。それ以外の場合、これらのリソースは VPC Connector セキュリティグループからのトラフィックを受け入れることができません。

> **Note**
>
> サービスを VPC に関連付けると、次のトラフィックは影響を受けません。
>
> - インバウンドトラフィック – アプリケーションが受信する受信メッセージは、関連付けられた VPC の影響を受けません。メッセージは、サービスに関連付けられているパブリックドメイン名を介してルーティングされ、VPC とやり取りしません。
> - App Runner トラフィック – App Runner は、ソースコードとイメージのプル、ログのプッシュ、シークレットの取得など、ユーザーに代わっていくつかのアクションを管理します。これらのアクションが生成するトラフィックは、VPC 経由でルーティングされません。

と Amazon VPC AWS App Runner の統合方法の詳細については、AWS 「App Runner VPC Networking」を参照してください。

> **Note**
>
> 送信トラフィックの場合、App Runner は現在 IPv4 のみをサポートしています。

VPC アクセスを管理する

> **Note**
>
> サービスのアウトバウンドトラフィック VPC コネクタを作成すると、次のサービス起動プロセスで 1 回限りのレイテンシーが発生します。この設定は、新しいサービスの作成時または作成後にサービスの更新で設定できます。詳細については、このガイド1 回限りのレイテンシーの「Networking with App Runner」の章の「」を参照してください。

次のいずれかの方法を使用して、App Runner サービスの VPC アクセスを管理します。

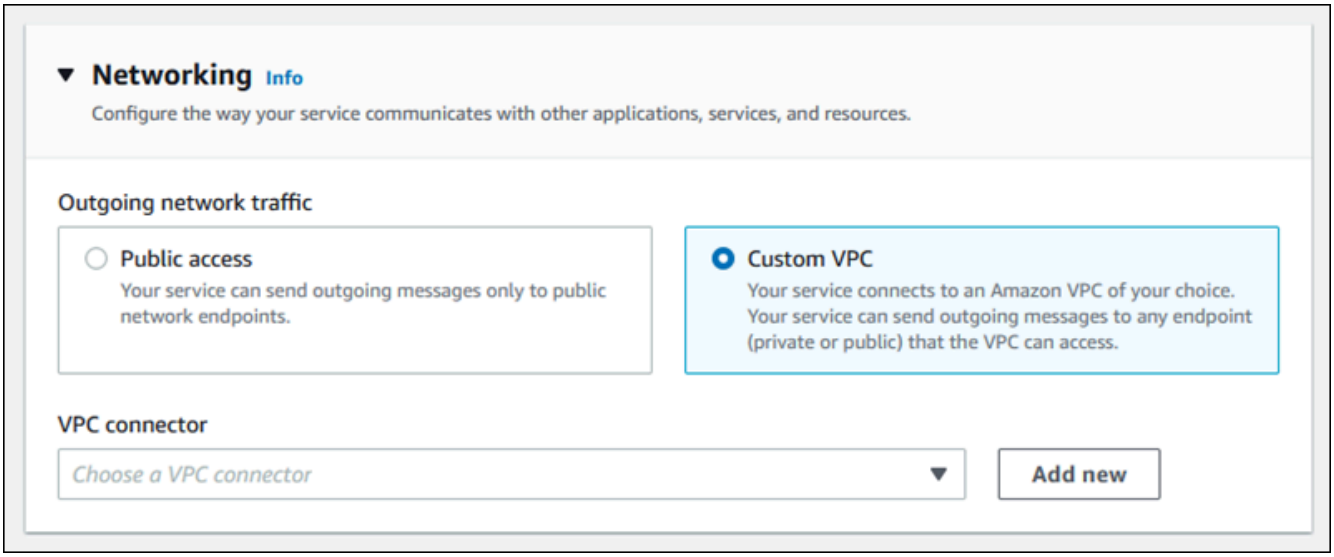
App Runner console

App Runner コンソールを使用してサービスを作成する場合、または後で設定を更新する場合は、送信トラフィックの設定を選択できます。コンソールページのネットワーク設定セクションを探します。送信ネットワークトラフィックでは、以下から選択します。

- パブリックアクセス: サービスを他の のパブリックエンドポイントに関連付ける。 AWS のサービス
- カスタム VPC: Amazon VPC から VPC にサービスを関連付けます。アプリケーションは に接続し、Amazon VPC でホストされている他のアプリケーションにメッセージを送信できます。

カスタム VPC を有効にするには

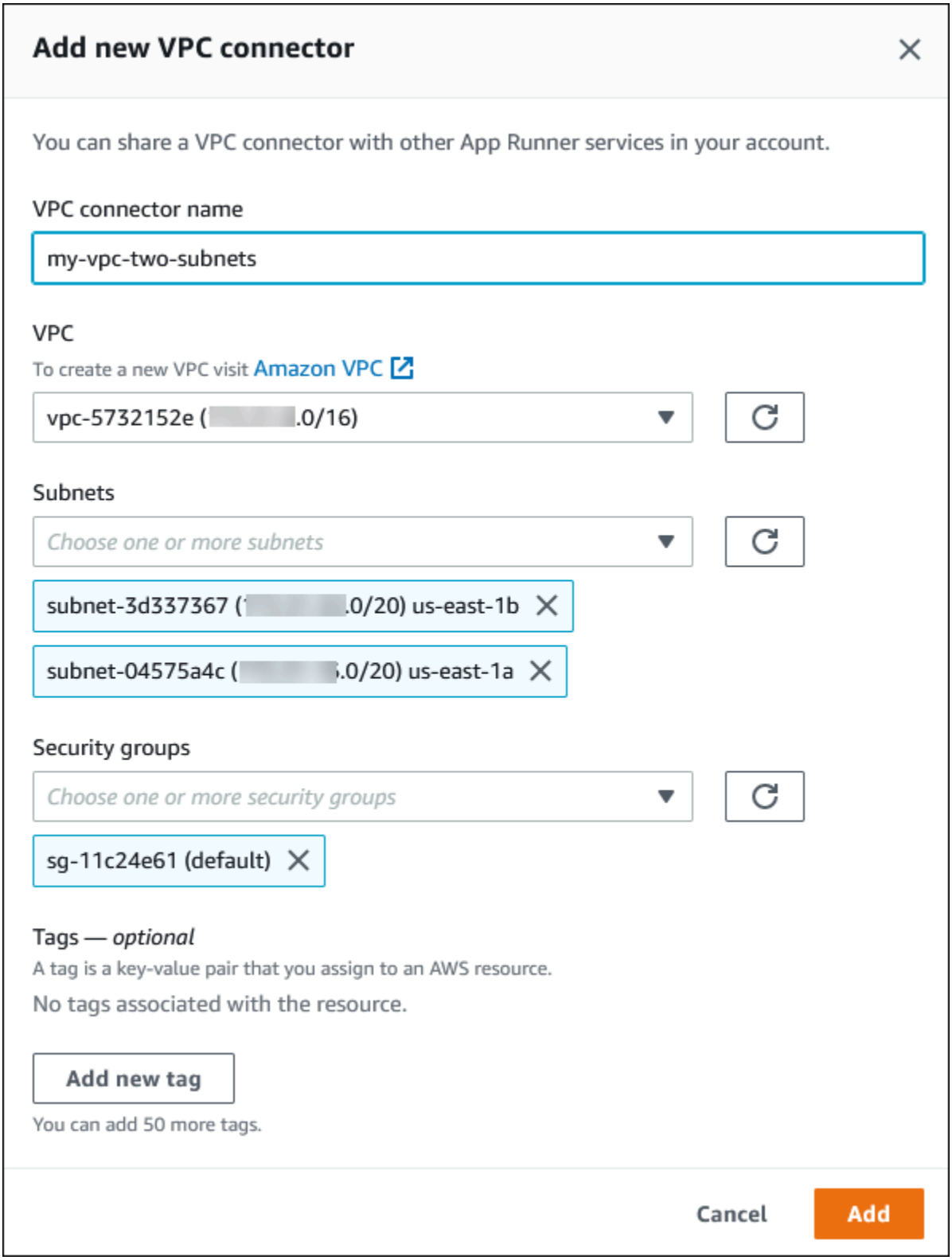
1. App Runner コンソールを開き、リージョンリストで を選択します AWS リージョン。
2. 「サービスの設定」の「ネットワーク」セクションに移動します。



3. 送信ネットワークトラフィックにカスタム VPC を選択します。
4. ナビゲーションペインで、VPC コネクタを選択します。

   VPC コネクタを作成した場合、コンソールにはアカウント内の VPC コネクタのリストが表示されます。既存の VPC コネクタを選択し、次へ を選択して設定を確認できます。次に、最後のステップに進みます。または、次の手順を使用して新しい VPC コネクタを追加することもできます。
5. 新規追加 を選択して、サービスの新しい VPC コネクタを作成します。

   次に、新しい VPC コネクタの追加ダイアログボックスが開きます。



6. VPC コネクタの名前を入力し、使用可能なリストから必要な VPC を選択します。

7. Subnets では、App Runner サービスにアクセスする予定のアベイラビリティーゾーンごとに 1 つのサブネットを選択します。可用性を高めるには、3 つのサブネットを選択します。または、サブネットが 3 つ未満の場合は、使用可能なすべてのサブネットを選択します。

> **Note**
>
> VPC コネクタにプライベートサブネットを割り当ててください。VPC コネクタにパブリックサブネットを割り当てると、更新中にサービスが自動的に作成またはロールバックされません。

8. (オプション) セキュリティグループで、エンドポイントネットワークインターフェイスに関連付けるセキュリティグループを選択します。
9. (オプション) タグを追加するには、[新しいタグを追加] を選択し、そのタグのキーと値を入力してください。
10. [追加] を選択します。

    作成した VPC コネクタの詳細は、VPC コネクタの下に表示されます。
11. 次へ を選択して設定を確認し、作成とデプロイを選択します。

    App Runner は VPC コネクタリソースを作成し、それをサービスに関連付けます。サービスが正常に作成されると、コンソールにサービスダッシュボードが表示され、新しいサービスの概要が表示されます。

App Runner API or AWS CLI

CreateService または UpdateService App Runner API アクションを呼び出すときは、`NetworkConfiguration`パラメータ`EgressConfiguration`のメンバーを使用して、サービスの VPC コネクタリソースを指定します。

次の App Runner API アクションを使用して、VPC Connector リソースを管理します。

- CreateVpcConnector – 新しい VPC コネクタを作成します。
- ListVpcConnectors – に関連付けられている VPC コネクタのリストを返します AWS アカウント。リストには詳細な説明が含まれています。
- DescribeVpcConnector – VPC コネクタの完全な説明を返します。
- DeleteVpcConnector – VPC コネクタを削除します。の VPC コネクタクォータに達した場合は AWS アカウント、不要な VPC コネクタを削除する必要がある場合があります。

VPC へのアウトバウンドアクセス権を持つアプリケーションを App Runner にデプロイするには、まず VPC コネクタを作成する必要があります。これを行うには、アプリケーションに関連付ける 1 つ以上のサブネットとセキュリティグループを指定します。その後、次の例に示すように、CLI を使用して Create または UpdateService で VPC Connector を参照できます。

```
            cat > vpc-connector.json <<EOF
{
"VpcConnectorName": "my-vpc-connector",
"Subnets": [
"subnet-a",
"subnet-b",
"subnet-c"
],
"SecurityGroups": [
"sg-1",
"sg-2"
]
}
EOF

aws apprunner create-vpc-connector \
--cli-input-json file:///vpc-connector.json

cat > service.json <<EOF

{
"ServiceName": "my-vpc-connected-service",
"SourceConfiguration": {
"ImageRepository": {
"ImageIdentifier": "<ecr-image-identifier> ",
"ImageConfiguration": {
"Port": "8000"
},
"ImageRepositoryType": "ECR"
}
},
"NetworkConfiguration": {
"EgressConfiguration": {
"EgressType": "VPC",
"VpcConnectorArn": "arn:aws:apprunner:..../my-vpc-connector"
}
}
```

```
}
EOF

aws apprunner create-service \
--cli-input-json file:///service.js
```

App Runner サービスのオブザーバビリティ

AWS App Runner は複数の AWS サービスと統合され、App Runner サービス用の広範なオブザーバビリティスイートを提供します。この章のトピックでは、これらの機能について説明します。

トピック

- App Runner サービスアクティビティの追跡
- CloudWatch Logs にストリーミングされた App Runner ログの表示
- CloudWatch にレポートされた App Runner サービスメトリクスの表示
- EventBridge での App Runner イベントの処理
- を使用した App Runner API コールのログ記録 AWS CloudTrail
- X-Ray を使用した App Runner アプリケーションのトレース

App Runner サービスアクティビティの追跡

AWS App Runner はオペレーションのリストを使用して、App Runner サービスのアクティビティを追跡します。オペレーションは、サービスの作成、設定の更新、サービスのデプロイなどの API アクションへの非同期呼び出しを表します。以下のセクションでは、App Runner コンソールおよび API を使用してアクティビティを追跡する方法を示します。

App Runner サービスアクティビティを追跡する

次のいずれかの方法を使用して、App Runner サービスアクティビティを追跡します。

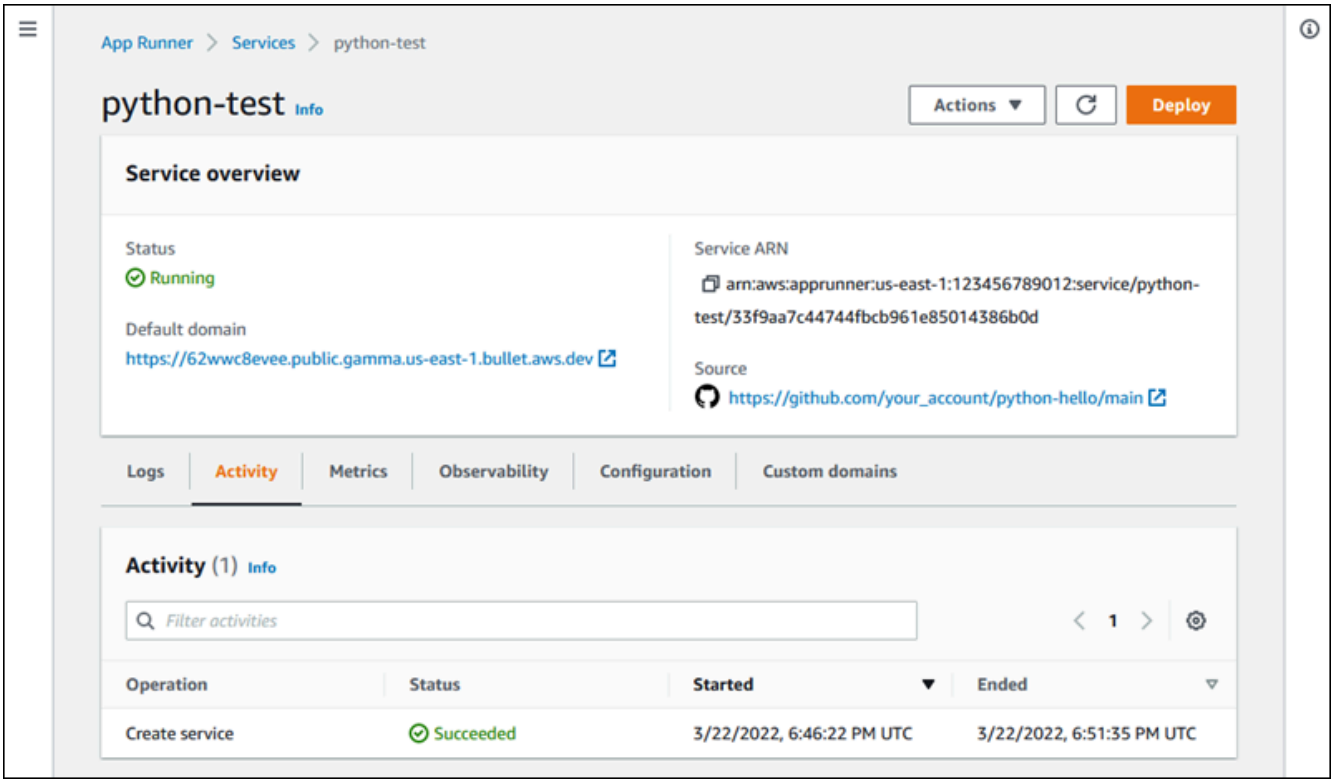
App Runner console

App Runner コンソールには、App Runner サービスアクティビティが表示され、オペレーションを調べるさまざまな方法が用意されています。

サービスのアクティビティを表示するには

1. App Runner コンソールを開き、リージョンリストで を選択します AWS リージョン。
2. ナビゲーションペインで、サービスを選択し、App Runner サービスを選択します。

   コンソールには、サービスダッシュボードにサービスの概要が表示されます。



3. サービスダッシュボードページで、まだ選択されていない場合はアクティビティタブを選択します。

   コンソールにオペレーションのリストが表示されます。

4. 特定のオペレーションを検索するには、検索語を入力してリストの範囲を絞り込みます。テーブルに表示される任意の値を検索できます。

5. リストされたオペレーションを選択して、関連するログを表示またはダウンロードします。

App Runner API or AWS CLI

ListOperations アクションは、App Runner サービスの Amazon リソースネーム (ARN) を指定して、このサービスで発生したオペレーションのリストを返します。各リスト項目には、オペレーション ID といくつかの追跡の詳細が含まれています。

CloudWatch Logs にストリーミングされた App Runner ログの表示

Amazon CloudWatch Logs を使用して、さまざまな AWS サービスのリソースが生成するログファイルをモニタリング、保存、およびアクセスできます。詳細については、Amazon CloudWatch Logs ユーザーガイドを参照してください。

AWS App Runner は、アプリケーションのデプロイとアクティブなサービスの出力を収集し、CloudWatch Logs にストリーミングします。以下のセクションでは、App Runner ログストリームを一覧表示し、App Runner コンソールでそれらを表示する方法を示します。

App Runner ロググループとストリーム

CloudWatch Logs はログデータをログストリームに保持し、さらにロググループに整理します。ログストリームは、特定のソースからの一連のログイベントです。ロググループは、保持、モニタリング、アクセス制御について同じ設定を共有するログストリームのグループです。

App Runner は、2 つの CloudWatch Logs ロググループを定義します。各ロググループは、 内の App Runner サービスごとに複数のログストリームを持ちます AWS アカウント。

サービスログ

サービスロググループには、App Runner サービスを管理し、それに対して動作するときに App Runner によって生成されたログ出力が含まれます。

ロググループ名	例
`/aws/apprunner/ service-name /service-id /service`	`/aws/apprunner/python-test/ac7ec8b51ff34746bcb6654e0bcb23da/service`

サービスロググループ内で、App Runner は App Runner サービスのライフサイクル内のアクティビティをキャプチャするイベントログストリームを作成します。たとえば、アプリケーションを起動したり、一時停止したりしている可能性があります。

さらに、App Runner は、サービスに関連する長時間実行される非同期オペレーションごとにログストリームを作成します。ログストリーム名には、オペレーションタイプと特定のオペレーション ID が反映されます。

デプロイはオペレーションの一種です。デプロイログには、サービスの作成時またはアプリケーションの新しいバージョンのデプロイ時に App Runner が実行するビルドおよびデプロイステップのログ出力が含まれます。デプロイログストリーム名は で始まりdeployment/、デプロイを実行するオペレーションの ID で終わります。このオペレーションは、最初のアプリケーションデプロイの場合は CreateService 呼び出し、それ以降のデプロイの場合は StartDeployment 呼び出しです。

デプロイログ内では、各ログメッセージはプレフィックスで始まります。

- [AppRunner] – デプロイ中に App Runner が生成する出力。
- [Build] – 独自のビルドスクリプトの出力。

ログストリーム名	例
events	該当なし (固定名)
operation-type /*operation-id*	deployment/c2c8eeedea164f459cf78f12a8953390

アプリケーションログ

アプリケーションロググループには、実行中のアプリケーションコードの出力が含まれます。

ロググループ名	例
/aws/apprunner/ *service-name* /*service-id* /application	/aws/apprunner/python-test/ac7ec8b51ff34746bcb6654e0bcb23da/application

App Runner は、アプリケーションロググループ内で、アプリケーションを実行しているインスタンス (スケーリングユニット) ごとにログストリームを作成します。

ログストリーム名	例
instance/ *instance-id*	instance/1a80bc9134a84699b7b3432ebeebb591

App Runner ロロロ

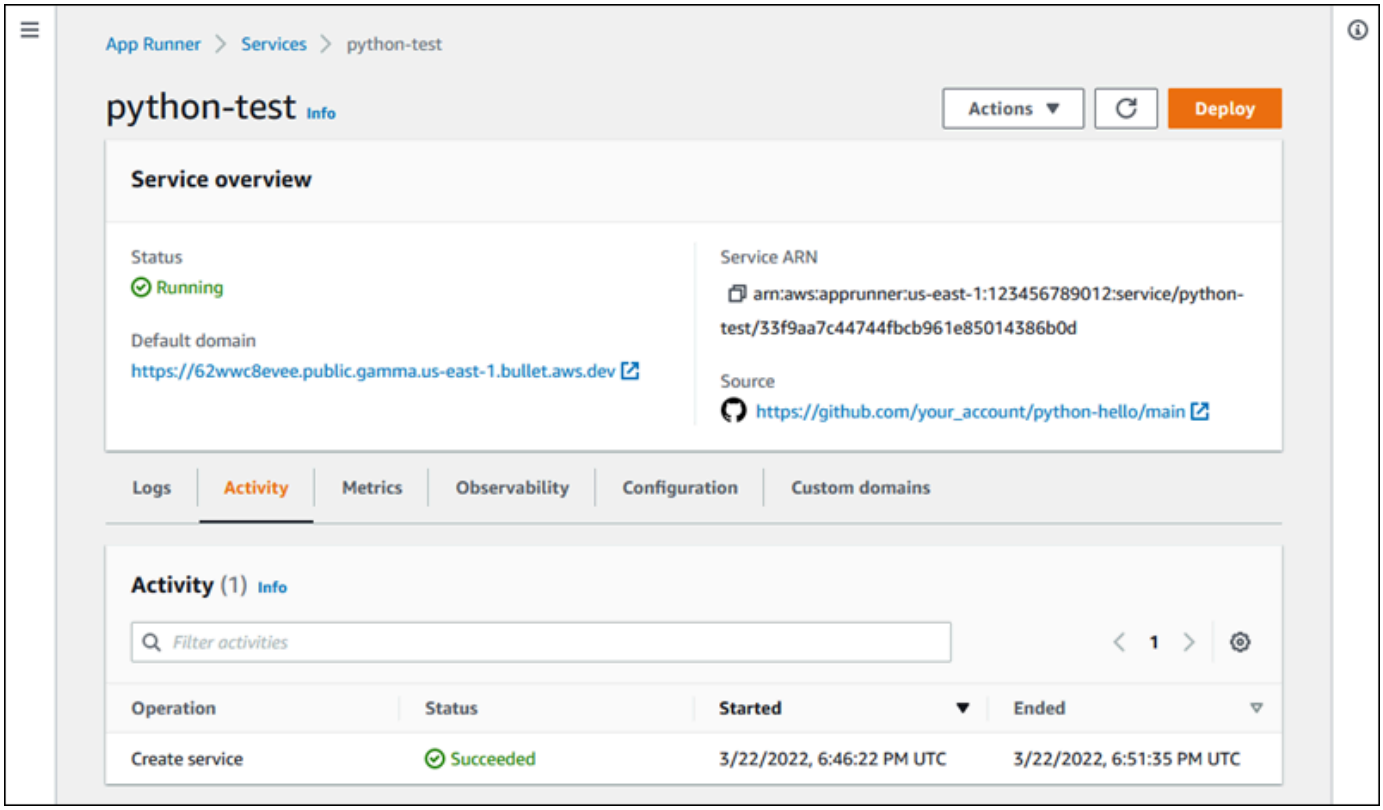
コンソールでの App Runner ログの表示

App Runner コンソールには、サービスのすべてのログの概要が表示され、それらのログを表示、探索、ダウンロードできます。

サービスのログを表示するには

1. App Runner コンソールを開き、リージョンリストで を選択します AWS リージョン。
2. ナビゲーションペインで、サービスを選択し、App Runner サービスを選択します。

   コンソールには、サービスダッシュボードにサービスの概要が表示されます。

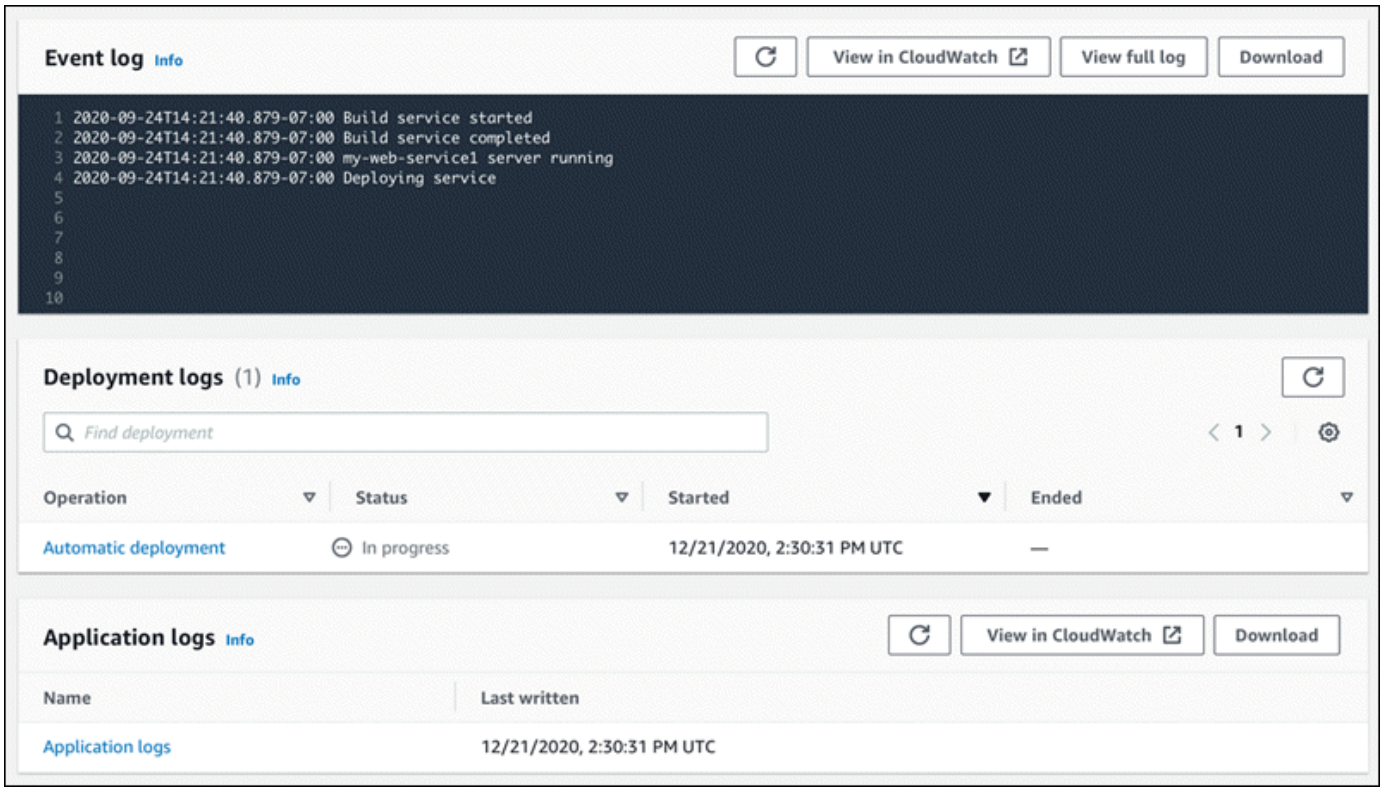


3. サービスダッシュボードページで、ログタブを選択します。

   コンソールには、いくつかのセクションにいくつかのタイプのログが表示されます。

   - イベントログ – App Runner サービスのライフサイクル内のアクティビティ。コンソールに最新のイベントが表示されます。
   - デプロイログ – App Runner サービスへのソースリポジトリのデプロイ。コンソールには、デプロイごとに個別のログストリームが表示されます。

- アプリケーションログ – App Runner サービスにデプロイされたウェブアプリケーションの出力。コンソールは、実行中のすべてのインスタンスからの出力を 1 つのログストリームに結合します。



4. 特定のデプロイを検索するには、検索語を入力してデプロイログリストの範囲を絞り込みます。テーブルに表示される任意の値を検索できます。
5. ログのコンテンツを表示するには、フルログの表示 (イベントログ) またはログストリーム名 (デプロイログとアプリケーションログ) を選択します。
6. ダウンロードを選択してログをダウンロードします。デプロイログストリームの場合は、まずログストリームを選択します。
7. CloudWatch で表示 を選択して CloudWatch コンソールを開き、その完全な機能を使用して App Runner サービスログを調べます。デプロイログストリームの場合は、まずログストリームを選択します。

> **Note**
>
> CloudWatch コンソールは、結合されたアプリケーションログではなく、特定のインスタンスのアプリケーションログを表示する場合に特に便利です。

CloudWatch にレポートされた App Runner サービスメトリクスの表示

Amazon CloudWatch は、Amazon Web Services (AWS) リソースと、 AWS で実行されているアプリケーションをリアルタイムでモニタリングします。CloudWatch を使用してメトリクスを収集および追跡できます。メトリクスとは、リソースやアプリケーションについて測定できる変数です。これを使用して、メトリクスを監視するアラームを作成することもできます。特定のしきい値に達すると、CloudWatch は通知を送信するか、モニタリング対象のリソースに自動的に変更を加えます。詳細については、「Amazon CloudWatch ユーザーガイド」を参照してください。

AWS App Runner は、App Runner サービスの使用状況、パフォーマンス、可用性をより詳細に可視化するさまざまなメトリクスを収集します。一部のメトリクスはウェブサービスを実行する個々のインスタンスを追跡しますが、その他のメトリクスはサービスレベル全体です。以下のセクションでは、App Runner メトリクスを一覧表示し、App Runner コンソールでそれらを表示する方法を示します。

App Runner メトリクス

App Runner は、サービスに関連する以下のメトリクスを収集し、 `AWS/AppRunner`名前空間の CloudWatch に発行します。

> **Note**
>
> 2023 年 8 月 23 日以前は、CPU 使用率とメモリ使用率のメトリクスは、現在計算されている使用率ではなく、vCPU ユニットと使用されたメモリのメガバイトに基づいていました。アプリケーションがこの日付より前に App Runner で実行され、戻って App Runner または CloudWatch コンソールでこの日付のメトリクスを表示するように選択した場合は、両方の単位のメトリクスが表示され、結果としていくつかの不規則性も表示されます。

> **Important**
>
> 2023 年 8 月 23 日より前に CPU 使用率とメモリ使用率のメトリクス値に基づく CloudWatch アラームを更新する必要があります。vCPU やメガバイトではなく使用率に基づいてトリガーするようにアラームを更新します。詳細については、「Amazon CloudWatch ユーザーガイド」を参照してください。

インスタンスレベルのメトリクスは、インスタンス (スケーリングユニット) ごとに個別に収集されます。

何を測定しますか？	メトリクス	説明
CPU utilization	`CPUUtilization`	サービス設定によって予約された CPU 使用率の合計のうち、1 分間の平均 CPU 使用率の割合。
Memory utilization	`MemoryUtilization`	サービス設定によって予約された合計メモリのうち、1 分間の平均メモリ使用量の割合。

サービスレベルのメトリクスは、サービス全体で収集されます。

何を測定しますか？	メトリクス	説明
CPU utilization	`CPUUtilization`	サービス設定によって予約された CPU 使用率の合計のうち、1 分間のすべてのインスタンスで集計された CPU 使用率の割合。
Memory utilization	`MemoryUtilization`	サービス設定によって予約された合計メモリのうち、1 分間のすべてのインスタンスでの合計メモリ使用量の割合。
Concurrency	`Concurrency`	サービスによって処理される同時リクエストのおおよその数。
HTTP request count	`Requests`	サービスが受信した HTTP リクエストの数。

HTTP status counts	`2xxStatusResponses`
	
	`4xxStatusResponses`
		カテゴリ (2XX、4XX, 5XX) 別にグループ化された、各レスポンスステータスを返した HTTP リクエストの数。

何を測定しますか？	メトリクス	説明
	`5xxStatusResponses`	
HTTP request latency	`RequestLatency`	ウェブサービスが HTTP リクエストを処理するのにかかったミリ秒単位の時間。
Instance counts	`ActiveInstances`	サービスの HTTP リクエストを処理しているインスタンスの数。 **Note** `ActiveInstances` メトリクスにゼロが表示された場合は、サービスに対するリクエストがないことを意味します。サービスのインスタンス数がゼロであることを示すものではありません。

コンソールでの App Runner メトリクスの表示

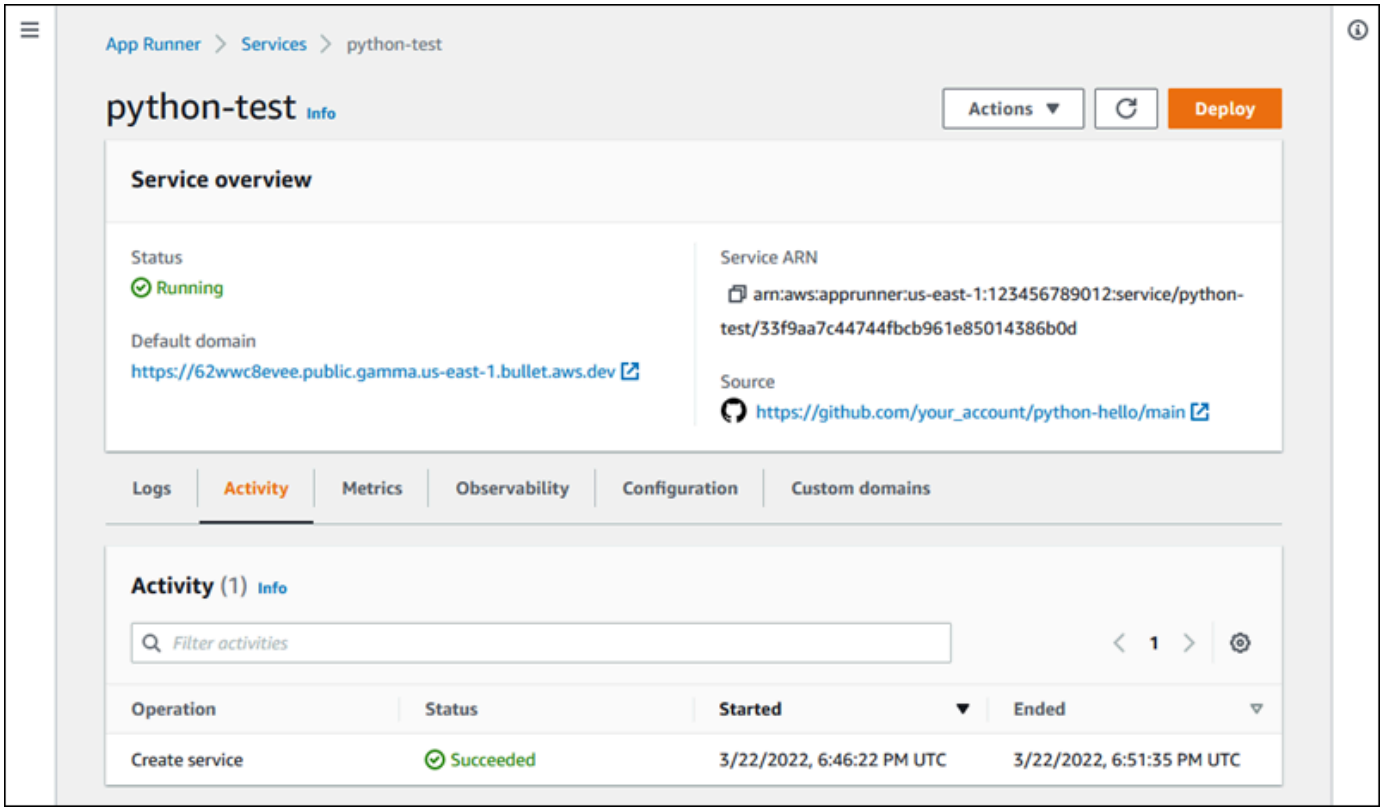
App Runner コンソールには、App Runner がサービス用に収集するメトリクスがグラフィカルに表示され、それらを探索するさまざまな方法が用意されています。

> **Note**
> 現時点では、コンソールにはサービスメトリクスのみが表示されます。インスタンスメトリクスを表示するには、CloudWatch コンソールを使用します。

サービスのログを表示するには

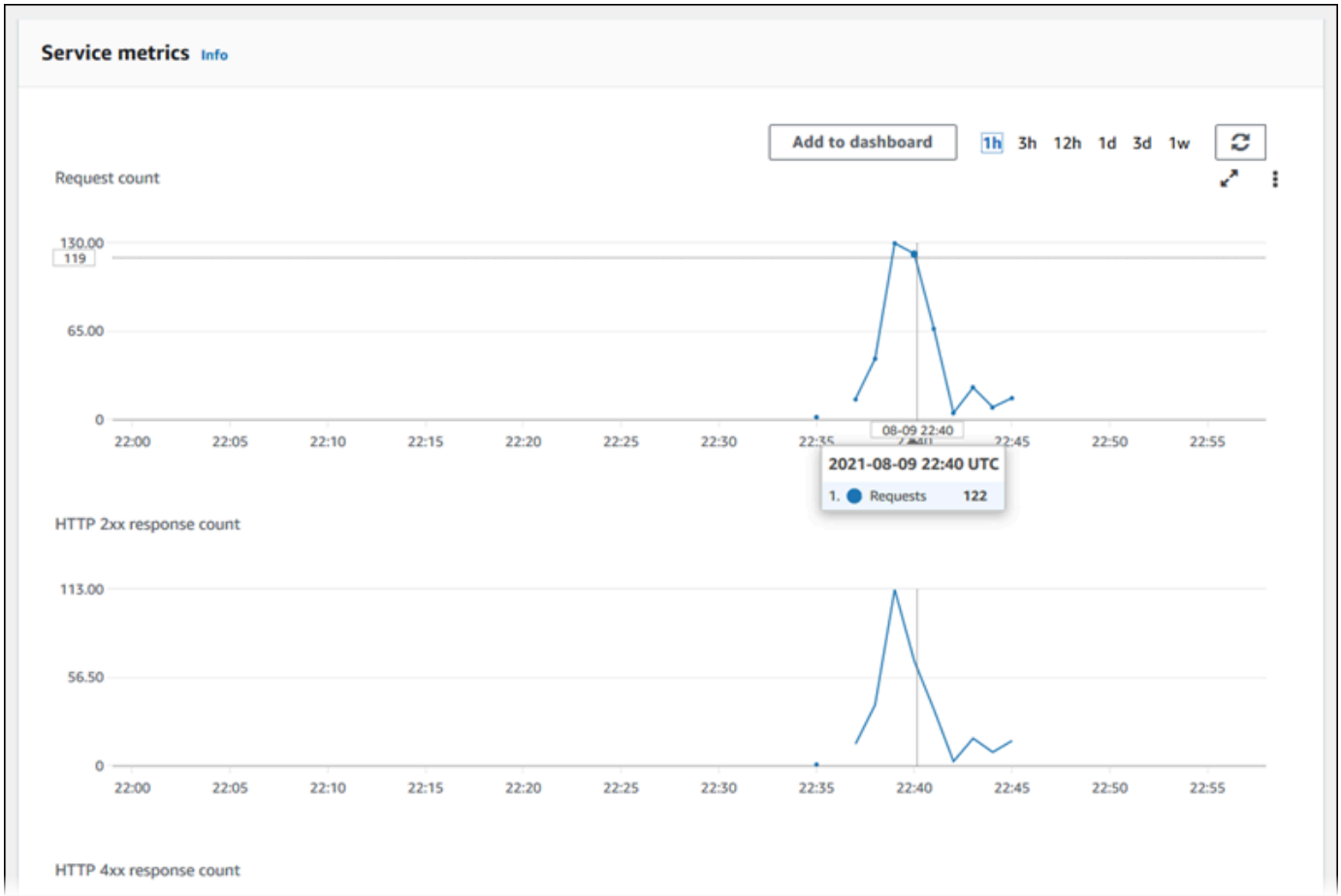
1. App Runner コンソールを開き、リージョンリストで を選択します AWS リージョン。
2. ナビゲーションペインで、サービスを選択し、App Runner サービスを選択します。

   コンソールには、サービスダッシュボードにサービスの概要が表示されます。



3. サービスダッシュボードページで、メトリクスタブを選択します。

   コンソールには、一連のメトリクスグラフが表示されます。



4. 期間 (12 時間など) を選択して、メトリクスグラフの範囲をその期間の最近の期間に設定します。
5. グラフセクションのいずれかの上部にあるダッシュボードに追加を選択するか、任意のグラフのメニューを使用して、CloudWatch コンソールのダッシュボードに関連メトリクスを追加して詳細に調査します。

EventBridge での App Runner イベントの処理

Amazon EventBridge を使用すると、特定のパターンについて AWS App Runner サービスからのリアルタイムデータのストリームをモニタリングするイベント駆動型ルールを設定できます。ルールのパターンが一致する AWS Batchと、EventBridge は Amazon ECS AWS Lambda、Amazon SNS などのターゲットでアクションを開始します。例えば、サービスへのデプロイが失敗するたびに Amazon SNS トピックにシグナルを送信することで、E メール通知を送信するためのルールを設定できます。または、サービスの更新が失敗した場合に Slack チャネルに通知するように Lambda 関数を設定できます。EventBridge の詳細については、「Amazon EventBridge ユーザーガイド」を参照してください。

App Runner が EventBridge に次のイベントタイプを送信する

- サービスステータスの変更 – App Runner サービスのステータスの変更。例えば、サービスのステータスが に変更されましたDELETE_FAILED。
- サービスオペレーションステータスの変更 – App Runner サービスでの長い非同期オペレーションのステータスの変更。例えば、サービスの作成が開始された、サービスの更新が正常に完了した、サービスデプロイがエラーで完了したなどです。

App Runner イベントを処理する EventBridge ルールの作成

EventBridge イベントは、ソース AWS サービスや詳細 (イベント) タイプ、イベントの詳細を含むイベント固有のフィールドのセットなど、一部の標準 EventBridge フィールドを定義するオブジェクトです。EventBridge ルールを作成するには、EventBridge コンソールを使用してイベントパターン (追跡する必要があるイベント) を定義し、ターゲットアクション (マッチングで実行する必要があるアクション) を指定します。イベントパターンは、一致するイベントに似ています。一致するフィールドのサブセットを指定し、各フィールドに対して、可能な値のリストを指定します。このトピックでは、App Runner イベントとイベントパターンの例を示します。

EventBridge ルールの作成の詳細については、「Amazon EventBridge ユーザーガイド」の AWS「 サービスのルールの作成」を参照してください。

> **Note**
>
> 一部のサービスは、EventBridge で事前定義されたパターンをサポートしています。これは、イベントパターンが作成される方法を簡素化します。フォーム上のフィールド値を選択すると、EventBridge がパターンを生成します。現時点では、App Runner は事前定義されたパターンをサポートしていません。パターンを JSON オブジェクトとして入力する必要があります。このトピックの例を出発点として使用できます。

App Runner イベントの例

以下は、App Runner が EventBridge に送信するイベントの例です。

- サービスステータス変更イベント。具体的には、 から RUNNINGステータスOPERATION_IN_PROGRESSに変更されたサービスです。

```
{
```

```
  "version": "0",
  "id": "6a7e8feb-b491-4cf7-a9f1-bf3703467718",
  "detail-type": "AppRunner Service Status Change",
  "source": "aws.apprunner",
  "account": "111122223333",
  "time": "2021-04-29T11:54:23Z",
  "region": "us-east-2",
  "resources": [
    "arn:aws:apprunner:us-east-2:123456789012:service/my-
app/8fe1e10304f84fd2b0df550fe98a71fa"
  ],
  "detail": {
    "previousServiceStatus": "OPERATION_IN_PROGRESS",
    "currentServiceStatus": "RUNNING",
    "serviceName": "my-app",
    "serviceId": "8fe1e10304f84fd2b0df550fe98a71fa",
    "message": "Service status is set to RUNNING.",
    "severity": "INFO"
  }
}
```

- オペレーションステータス変更イベント。具体的には、正常に完了したUpdateServiceオペレーションです。

```
{
  "version": "0",
  "id": "6a7e8feb-b491-4cf7-a9f1-bf3703467718",
  "detail-type": "AppRunner Service Operation Status Change",
  "source": "aws.apprunner",
  "account": "111122223333",
  "time": "2021-04-29T18:43:48Z",
  "region": "us-east-2",
  "resources": [
    "arn:aws:apprunner:us-east-2:123456789012:service/my-
app/8fe1e10304f84fd2b0df550fe98a71fa"
  ],
  "detail": {
    "operationStatus": "UpdateServiceCompletedSuccessfully",
    "serviceName": "my-app",
    "serviceId": "8fe1e10304f84fd2b0df550fe98a71fa",
    "message": "Service update completed successfully. New application and
 configuration is deployed.",
    "severity": "INFO"
```

```
  }
}
```

App Runner イベントパターンの例

次の例は、1 つ以上の App Runner イベントを照合するために EventBridge ルールで使用できるイベントパターンを示しています。イベントパターンはイベントに似ています。一致させるフィールドのみを含め、それぞれにスカラーの代わりにリストを指定します。

- 特定のアカウントのサービスのすべてのサービスステータス変更イベントをマッチングします。サービスのステータスはなくなりましたRUNNING。

```
{
  "detail-type": [ "AppRunner Service Status Change" ],
  "source": [ "aws.apprunner" ],
  "account": [ "111122223333" ],
  "detail": {
    "previousServiceStatus": [ "RUNNING" ]
  }
}
```

- オペレーションが失敗した特定のアカウントのサービスのオペレーションステータス変更イベントをすべて一致させます。

```
{
  "detail-type": [ "AppRunner Service Operation Status Change" ],
  "source": [ "aws.apprunner" ],
  "account": [ "111122223333" ],
  "detail": {
    "operationStatus": [
      "CreateServiceFailed",
      "DeleteServiceFailed",
      "UpdateServiceFailed",
      "DeploymentFailed",
      "PauseServiceFailed",
      "ResumeServiceFailed"
    ]
  }
}
```

App Runner イベントリファレンス

サービスステータスの変更

サービスステータス変更イベントが にdetail-type設定されていますAppRunner Service Status Change。次の詳細フィールドと値があります。

```
"serviceId": "your service ID",
"serviceName": "your service name",
"message": "Service status is set to CurrentStatus.",
"previousServiceStatus": "any valid service status",
"currentServiceStatus": "any valid service status",
"severity": "varies"
```

オペレーションステータスの変更

オペレーションステータスの変更イベントが にdetail-type設定されていますAppRunner Service Operation Status Change。次の詳細フィールドと値があります。

```
"operationStatus": "see following table",
"serviceName": "your service name",
"serviceId": "your service ID",
"message": "see following table",
"severity": "varies"
```

次の表に、すべてのステータスコードと関連するメッセージを示します。

ステータス	メッセージ
CreateServiceStarted	サービスの作成が開始されました。
CreateServiceCompletedSuccessfully	サービスの作成が正常に完了しました。
CreateServiceFailed	サービスの作成に失敗しました。詳細については、「 サービスログ」を参照してください。
DeleteServiceStarted	サービスの削除が開始されました。

ステータス	メッセージ
DeleteServiceCompletedSuccessfully	サービスの削除が正常に完了しました。
DeleteServiceFailed	サービスの削除に失敗しました。
UpdateServiceStarted	
UpdateServiceCompletedSuccessfully	サービスの更新が正常に完了しました。新しいアプリケーションと設定がデプロイされます。
	サービスの更新が正常に完了しました。新しい設定がデプロイされます。
UpdateServiceFailed	サービスの更新に失敗しました。詳細については、「 サービスログ」を参照してください。
DeploymentStarted	デプロイが開始されました。
DeploymentCompletedSuccessfully	デプロイが正常に完了しました。
DeploymentFailed	デプロイに失敗しました。詳細については、「 サービスログ」を参照してください。
PauseServiceStarted	サービスの一時停止が開始されました。
PauseServiceCompletedSuccessfully	サービスの一時停止が正常に完了しました。
PauseServiceFailed	サービスの一時停止に失敗しました。
ResumeServiceStarted	サービス再開が開始されました。
ResumeServiceCompletedSuccessfully	サービス再開が正常に完了しました。
ResumeServiceFailed	サービス再開に失敗しました。

を使用した App Runner API コールのログ記録 AWS CloudTrail

App Runner は AWS CloudTrail、App Runner のユーザー、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、App Runner 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、App Runner コンソールからの呼び出しと、App Runner API オペレーションへのコード呼び出しが含まれます。証跡を作成する場合は、App Runner 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 で収集された情報を使用して、App Runner 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。

CloudTrail の詳細については、「AWS CloudTrail ユーザーガイド」を参照してください。

CloudTrail の App Runner 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。App Runner 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、「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。

App Runner 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より詳細に分析し、それに基づいて行動するように、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:

- 証跡の作成のための概要
- CloudTrail がサポートするサービスと統合
- CloudTrail 用 Amazon SNS 通知の構成
- 「複数のリージョンからCloudTrailログファイルを受け取る」および「複数のアカウントから CloudTrailログファイルを受け取る」

すべての App Runner アクションは CloudTrail によってログに記録され、 AWS App Runner API リファレンスに記載されています。例えば、`CreateService`、`DeleteConnection`、`StartDeployment` の各アクションを呼び出すと、CloudTrail ログファイルにエントリが生成されます。

各イベントまたはログエントリには、リクエストの生成者に関する情報が含まれます。同一性情報は次の判断に役立ちます。

- リクエストが、ルートと IAM ユーザー認証情報のどちらを使用して送信されたか。
- リクエストがロールまたはフェデレーションユーザーの一時的なセキュリティ認証情報を使用して行われたかどうか。
- リクエストが別の AWS サービスによって行われたかどうか。

詳細については、CloudTrail userIdentity 要素を参照してください。

App Runner ログファイルエントリについて

「トレイル」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 のログファイルには、ログエントリが 1 つ以上あります。イベントは、あらゆるソース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、およびリクエストパラメータに関する情報が含まれています。CloudTrail ログファイルは、パブリック API コール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。

以下の例は、`CreateService` アクションを示す CloudTrail ログエントリです。

> **Note**
>
> セキュリティ上の理由から、一部のプロパティ値はログで編集され、テキスト に置き換えられます`HIDDEN_DUE_TO_SECURITY_REASONS`。これにより、シークレット情報が意図せず公開されるのを防ぐことができます。ただし、これらのプロパティがリクエストで渡されたか、レスポンスで返されたことは依然として確認できます。

`CreateService` App Runner アクションの CloudTrail ログエントリの例

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "IAMUser",
```

```
    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
    "arn": "arn:aws:iam::123456789012:user/aws-user",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "userName": "aws-user"
  },
  "eventTime": "2020-10-02T23:25:33Z",
  "eventSource": "apprunner.amazonaws.com",
  "eventName": "CreateService",
  "awsRegion": "us-east-2",
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_6) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/77.0.3865.75 Safari/537.36",
  "requestParameters": {
    "serviceName": "python-test",
    "sourceConfiguration": {
      "codeRepository": {
        "repositoryUrl": "https://github.com/github-user/python-hello",
        "sourceCodeVersion": {
          "type": "BRANCH",
          "value": "main"
        },
        "codeConfiguration": {
          "configurationSource": "API",
          "codeConfigurationValues": {
            "runtime": "python3",
            "buildCommand": "HIDDEN_DUE_TO_SECURITY_REASONS",
            "startCommand": "HIDDEN_DUE_TO_SECURITY_REASONS",
            "port": "8080",
            "runtimeEnvironmentVariables": "HIDDEN_DUE_TO_SECURITY_REASONS"
          }
        }
      },
      "autoDeploymentsEnabled": true,
      "authenticationConfiguration": {
        "connectionArn": "arn:aws:apprunner:us-east-2:123456789012:connection/your-
connection/e7656250f67242d7819feade6800f59e"
      }
    },
    "healthCheckConfiguration": {
      "protocol": "HTTP"
    },
    "instanceConfiguration": {
      "cpu": "256",
```

```
      "memory": "1024"
    }
  },
  "responseElements": {
    "service": {
        "serviceName": "python-test",
        "serviceId": "dfa2b7cc7bcb4b6fa6c1f0f4efff988a",
        "serviceArn": "arn:aws:apprunner:us-east-2:123456789012:service/python-test/
dfa2b7cc7bcb4b6fa6c1f0f4efff988a",
        "serviceUrl": "generated domain",
        "createdAt": "2020-10-02T23:25:32.650Z",
        "updatedAt": "2020-10-02T23:25:32.650Z",
        "status": "OPERATION_IN_PROGRESS",
        "sourceConfiguration": {
            "codeRepository": {
                "repositoryUrl": "https://github.com/github-user/python-hello",
                "sourceCodeVersion": {
                    "type": "Branch",
                    "value": "main"
                },
                "sourceDirectory": "/",
                "codeConfiguration": {
                    "codeConfigurationValues": {
                        "configurationSource": "API",
                        "runtime": "python3",
                        "buildCommand": "HIDDEN_DUE_TO_SECURITY_REASONS",
                        "startCommand": "HIDDEN_DUE_TO_SECURITY_REASONS",
                        "port": "8080",
                        "runtimeEnvironmentVariables": "HIDDEN_DUE_TO_SECURITY_REASONS"
                    }
                }
            },
            "autoDeploymentsEnabled": true,
            "authenticationConfiguration": {
                "connectionArn": "arn:aws:apprunner:us-east-2:123456789012:connection/
your-connection/e7656250f67242d7819feade6800f59e"
            }
        },
        "healthCheckConfiguration": {
            "protocol": "HTTP",
            "path": "/",
            "interval": 5,
            "timeout": 2,
            "healthyThreshold": 3,
```

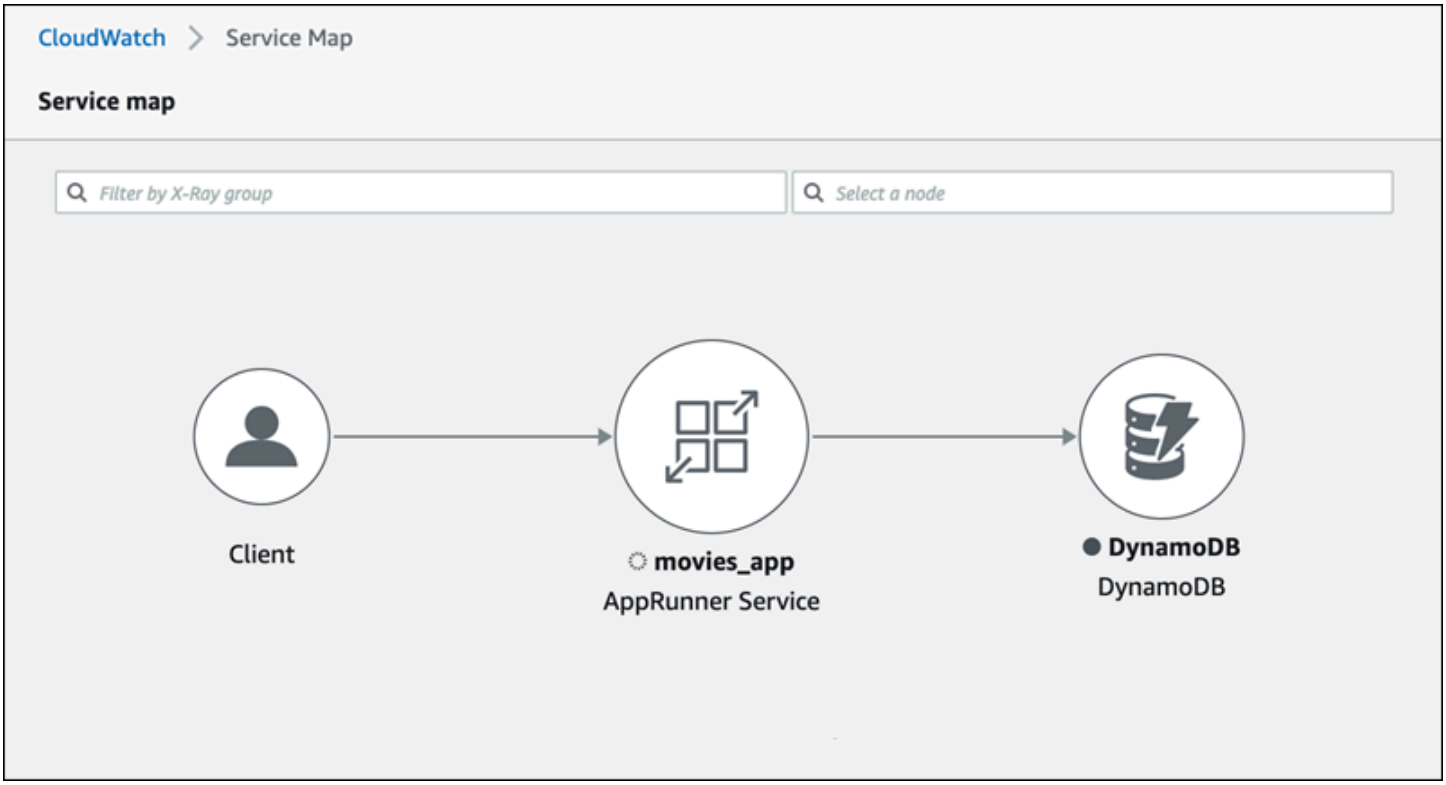
```
            "unhealthyThreshold": 5
        },
        "instanceConfiguration": {
            "cpu": "256",
            "memory": "1024"
        },
        "autoScalingConfigurationSummary": {
            "autoScalingConfigurationArn": "arn:aws:apprunner:us-
east-2:123456789012:autoscalingconfiguration/
DefaultConfiguration/1/00000000000000000000000000000001",
            "autoScalingConfigurationName": "DefaultConfiguration",
            "autoScalingConfigurationRevision": 1
        }
    }
},
  "requestID": "1a60af60-ecf5-4280-aa8f-64538319ba0a",
  "eventID": "e1a3f623-4d24-4390-a70b-bf08a0e24669",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "recipientAccountId": "123456789012"
}
```


X-Ray を使用した App Runner アプリケーションのトレース

AWS X-Ray は、アプリケーションが処理するリクエストに関するデータを収集するサービスであり、そのデータを表示、フィルタリング、インサイトを取得して、問題や最適化の機会を特定するために使用できるツールを提供します。アプリケーションへのトレースされたリクエストについては、リクエストとレスポンスだけでなく、アプリケーションがダウンストリーム AWS リソース、マイクロサービス、データベース、HTTP ウェブ APIs に対して行う呼び出しに関する詳細情報も確認できます。

X-Ray は、クラウドアプリケーションを強化する AWS リソースからのトレースデータを使用して、詳細なサービスグラフを生成します。サービスグラフには、フロントエンドサービスが呼び出してリクエストを処理しデータを維持するクライアント、フロントエンドサービス、バックエンドサービスが表示されます。サービスグラフを使用して、ボトルネック、レイテンシーのスパイク、その他の問題を識別して解決し、アプリケーションのパフォーマンスを向上させます。

X-Ray の詳細については、「AWS X-Ray デベロッパーガイド」を参照してください。



トレース用にアプリケーションを計測する

ポータブルテレメトリ仕様である OpenTelemetry を使用して、App Runner サービスアプリケーションをトレース用に計測します。現時点では、App Runner は AWS Distro for OpenTelemetry (ADOT) をサポートしています。ADOT は、 AWS サービスを使用してテレメトリ情報を収集して表示する OpenTelemetry 実装です。X-Ray はトレースコンポーネントを実装します。

アプリケーションで使用する特定の ADOT SDK に応じて、ADOT は自動と手動の 2 つの計測アプローチをサポートします。SDK を使用した計測の詳細については、ADOT ドキュメントを参照し、ナビゲーションペインで SDK を選択します。

ランタイム設定

App Runner サービスアプリケーションをトレース用に計測するための一般的なランタイムセットアップ手順は次のとおりです。

ランタイムのトレースを設定するには

1. AWS Distro for OpenTelemetry (ADOT) のランタイムに用意されている手順に従って、アプリケーションを計測します。

2. ソースコードリポジトリを使用している場合は `apprunner.yaml`ファイルの `build`セクションに、コンテナイメージを使用している場合は Dockerfile に必要な`OTEL`依存関係をインストールします。
3. ソースコードリポジトリを使用している場合は `apprunner.yaml` ファイルで、コンテナイメージを使用している場合は Dockerfile で環境変数を設定します。

   Example 環境変数

> **Note**
>
> 次の の例では、 `apprunner.yaml` ファイルに追加する重要な環境変数を一覧表示します。コンテナイメージを使用している場合は、これらの環境変数を Dockerfile に追加します。ただし、各ランタイムには独自のイディオシンクレーシーがあり、次のリストに環境変数を追加する必要がある場合があります。ランタイム固有の手順とランタイム用にアプリケーションをセットアップする方法の例の詳細については、AWS 「 Distro for OpenTelemetry」を参照して、「開始方法」の「ランタイム」を参照してください。

```
env:
    - name: OTEL_PROPAGATORS
      value: xray
    - name: OTEL_METRICS_EXPORTER
      value: none
    - name: OTEL_EXPORTER_OTLP_ENDPOINT
      value: http://localhost:4317
    - name: OTEL_RESOURCE_ATTRIBUTES
      value: 'service.name=example_app'
```

> **Note**
>
> `OTEL_METRICS_EXPORTER=none` App Runner Otel コレクターはメトリクスのログ記録を受け入れないため、 は App Runner にとって重要な環境変数です。メトリクスのトレースのみを受け入れます。

ランタイムセットアップの例

次の例は、ADOT Python SDK を使用してアプリケーションを自動計測する方法を示しています。SDK は、アプリケーションの Python フレームワークで使用される値を記述するテレメトリデータを含むスパンを自動的に生成します。Python コードを 1 行追加する必要はありません。2 つのソースファイルで数行のみを追加または変更する必要があります。

まず、次の例に示すように、いくつかの依存関係を追加します。

Example requirements.txt

```
opentelemetry-distro[otlp]>=0.24b0
opentelemetry-sdk-extension-aws~=2.0
opentelemetry-propagator-aws-xray~=1.0
```

次に、アプリケーションを計測します。これを行う方法は、ソースイメージまたはソースコードなどのサービスソースによって異なります。

Source image

サービスソースがイメージの場合、コンテナイメージの構築とイメージ内のアプリケーションの実行を制御する Dockerfile を直接計測できます。次の例は、Python アプリケーションの計測された Dockerfile を示しています。インストルメンテーションの追加は太字で強調されます。

Example Dockerfile

```
FROM public.ecr.aws/amazonlinux/amazonlinux:latest
RUN yum install python3.7 -y && curl -O https://bootstrap.pypa.io/get-pip.py &&
 python3 get-pip.py && yum update -y
COPY . /app
WORKDIR /app
RUN pip3 install -r requirements.txt
RUN opentelemetry-bootstrap --action=install
ENV OTEL_PYTHON_DISABLED_INSTRUMENTATIONS=urllib3
ENV OTEL_METRICS_EXPORTER=none
ENV OTEL_RESOURCE_ATTRIBUTES='service.name=example_app'
CMD OTEL_PROPAGATORS=xray OTEL_PYTHON_ID_GENERATOR=xray opentelemetry-instrument
 python3 app.py
EXPOSE 8080
```

Source code repository

サービスソースがアプリケーションソースを含むリポジトリである場合は、App Runner 設定ファイル設定を使用してイメージを間接的に計測します。これらの設定は、アプリケーションのイメージを構築するために App Runner が生成および使用する Dockerfile を制御します。次の例は、Python アプリケーション用に実装された App Runner 設定ファイルを示しています。インストルメンテーションの追加は太字で強調されます。

Example apprunner.yaml

```
version: 1.0
runtime: python3
build:
  commands:
    build:
      - pip install -r requirements.txt
      - opentelemetry-bootstrap --action=install
run:
  command: opentelemetry-instrument python app.py
  network:
    port: 8080
  env:
    - name: OTEL_PROPAGATORS
      value: xray
    - name: OTEL_METRICS_EXPORTER
      value: none
    - name: OTEL_PYTHON_ID_GENERATOR
      value: xray
    - name: OTEL_PYTHON_DISABLED_INSTRUMENTATIONS
      value: urllib3
    - name: OTEL_RESOURCE_ATTRIBUTES
      value: 'service.name=example_app'
```

App Runner サービスインスタンスロールに X-Ray アクセス許可を追加する

App Runner サービスで X-Ray トレースを使用するには、サービスのインスタンスに X-Ray サービスとやり取りするためのアクセス許可を付与する必要があります。これを行うには、インスタンスロールをサービスに関連付け、X-Ray アクセス許可を持つ管理ポリシーを追加します。App Runner インスタンスロールの詳細については、「」を参照してくださいthe section called “インスタンス

ロール”。`AWSXRayDaemonWriteAccess` マネージドポリシーをインスタンスロールに追加し、作成時にサービスに割り当てます。

App Runner サービスの X-Ray トレースを有効にする

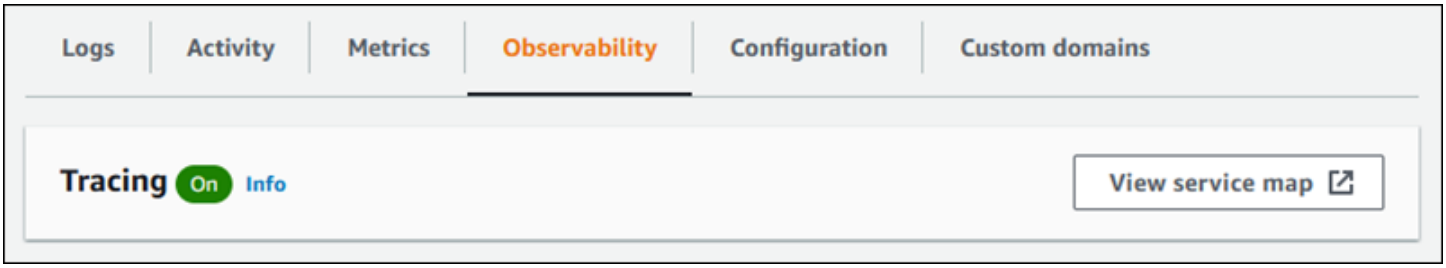
サービスを作成すると、App Runner はデフォルトでトレースを無効にします。オブザーバビリティの設定の一環として、サービスの X-Ray トレースを有効にできます。詳細については、「the section called “オブザーバビリティの管理”」を参照してください。

App Runner API または を使用する場合 AWS CLI、TraceConfigurationオブジェクト内の TraceConfiguration オブジェクトにはトレース設定が含まれます。 ObservabilityConfiguration トレースを無効にしたままにするには、 `TraceConfiguration` オブジェクトを指定しないでください。

コンソールと API の両方のケースで、前のセクションで説明したインスタンスロールを App Runner サービスに関連付けてください。

App Runner サービスの X-Ray トレースデータを表示する

App Runner コンソールのサービスダッシュボードページのオブザーバビリティタブで、サービスマップを表示を選択して Amazon CloudWatch コンソールに移動します。



Amazon CloudWatch コンソールを使用して、アプリケーションが処理するリクエストのサービスマップとトレースを表示します。サービスマップには、リクエストのレイテンシーや、他のアプリケーションや AWS サービスとのやり取りなどの情報が表示されます。コードに追加するカスタム注釈を使用すると、トレースを簡単に検索できます。詳細については、Amazon CloudWatch ユーザーガイド」のServiceLens を使用してアプリケーションの状態をモニタリングする」を参照してください。

AWS WAF ウェブ ACL をサービスに関連付ける

AWS WAF は、App Runner サービスを保護するために使用できるウェブアプリケーションファイアウォールです。 AWS WAF ウェブアクセスコントロールリスト (ウェブ ACLs) を使用すると、一般的なウェブエクスプロイトや不要なボットから App Runner サービスエンドポイントを保護できます。

ウェブ ACL を使用すると、App Runner サービスへのすべての受信ウェブリクエストをきめ細かく制御できます。ウェブトラフィックを許可、ブロック、またはモニタリングするルールをウェブ ACL で定義して、承認された正当なリクエストのみがウェブアプリケーションと APIs に到達するようにすることができます。特定のビジネスおよびセキュリティのニーズに基づいて、ウェブ ACL ルールをカスタマイズできます。ネットワーク ACLs「ネットワークトラフィックの制御」を参照してください。

> **Important**
>
> WAF ウェブ ACLsルールは、IP ベースのルールに準拠していません。これは、現在、リクエストソース IP データの WAF に関連付けられた App Runner プライベートサービスへの転送をサポートしていないためです。App Runner アプリケーションにソース IP/CIDR 受信トラフィックコントロールルールが必要な場合は、WAF ウェブ ACLs の代わりにプライベートエンドポイントのセキュリティグループルールを使用する必要があります。

受信ウェブリクエストフロー

AWS WAF ウェブ ACL が App Runner サービスに関連付けられている場合、受信ウェブリクエストは次のプロセスを実行します。

1. App Runner はオリジンリクエストの内容を に転送します AWS WAF。
2. AWS WAF はリクエストを検査し、その内容をウェブ ACL で指定したルールと比較します。
3. その検査に基づいて、 は App Runner に `allow`または `block`レスポンス AWS WAF を返します。
   - `allow` レスポンスが返された場合、App Runner はリクエストをアプリケーションに転送します。

- `block` レスポンスが返された場合、App Runner はリクエストがウェブアプリケーションに到達するのをブロックします。レスポンスを `block`からアプリケーションに転送 AWS WAF します。

> **Note**
>
> デフォルトでは、応答が返されない場合、App Runner はリクエストをブロックします AWS WAF。

AWS WAF ウェブ ACLs「 AWS WAF デベロッパーガイド」の「ウェブアクセスコントロールリスト (ウェブ ACLs」を参照してください。

> **Note**
>
> 標準 AWS WAF 料金が発生します。App Runner サービスで AWS WAF ウェブ ACLs を使用しても、追加料金は発生しません。
> 料金の詳細については、AWS WAF 「 料金表」を参照してください。

WAF ウェブ ACLs App Runner サービスに関連付ける

AWS WAF ウェブ ACL を App Runner サービスに関連付ける大まかなプロセスを次に示します。

1. AWS WAF コンソールでウェブ ACL を作成します。詳細については、「 デベロッパーガイド」の「ウェブ ACL の作成」を参照してください。 AWS WAF
2. の AWS Identity and Access Management (IAM) アクセス許可を更新します AWS WAF。詳細については、「 アクセス許可」を参照してください。
3. 次のいずれかの方法を使用して、ウェブ ACL を App Runner サービスに関連付けます。
   - App Runner コンソール: App Runner サービスを作成または更新するときに、App Runner コンソールを使用して既存のウェブ ACL を関連付けます。手順については、AWS WAF 「ウェブ ACLs」を参照してください。
   - AWS WAF コンソール: 既存の App Runner サービスの AWS WAF コンソールを使用してウェブ ACL を関連付けます。詳細については、「AWS WAF デベロッパーガイド」の「ウェブ ACL と AWS リソースの関連付けまたは関連付け解除」を参照してください。

- AWS CLI: AWS WAF パブリック APIs。 AWS WAF パブリック APIs「 API AWS WAF リファレンスガイド」のAssociateWebACL」を参照してください。

考慮事項

- WAF ウェブ ACLsルールは、IP ベースのルールに準拠していません。これは、現在、リクエストソース IP データの WAF に関連付けられた App Runner プライベートサービスへの転送をサポートしていないためです。App Runner アプリケーションにソース IP/CIDR 受信トラフィックコントロールルールが必要な場合は、WAF ウェブ ACLs の代わりにプライベートエンドポイントのセキュリティグループルールを使用する必要があります。
- App Runner サービスは、1 つのウェブ ACL にのみ関連付けることができます。ただし、1 つのウェブ ACL を複数の App Runner サービスおよび複数の AWS リソースに関連付けることができます。例としては、Amazon Cognito ユーザープールや Application Load Balancer リソースなどがあります。
- ウェブ ACL を作成すると、ウェブ ACL が完全に伝播され、App Runner で使用できるようになるまでに少し時間がかかります。伝達時間は数秒から数分までです。ウェブ ACL が完全に伝達される前に関連付けようと`WAFUnavailableEntityException`すると、 は AWS WAF を返します。

  ウェブ ACL が完全に伝播される前にブラウザを更新したり、App Runner コンソールから移動したりすると、関連付けは失敗します。ただし、App Runner コンソール内を移動することはできます。
- AWS WAF は、無効な状態の App Runner サービスに対して次のいずれか AWS WAF APIs を呼び出すと、`WAFNonexistentItemException`エラーを返します。
  - `AssociateWebACL`
  - `DisassociateWebACL`
  - `GetWebACLForResource`

  App Runner サービスの無効な状態は次のとおりです。
  - `CREATE_FAILED`
  - `DELETE_FAILED`
  - `DELETED`
  - `OPERATION_IN_PROGRESS`

> **Note**
>
> `OPERATION_IN_PROGRESS` 状態は、App Runner サービスが削除されている場合にのみ無効になります。

- リクエストにより、 が検査 AWS WAF できるペイロードの制限を超える可能性があります。が App Runner からのオーバーサイズリクエスト AWS WAF を処理する方法の詳細については、「AWS WAF デベロッパーガイド」の「オーバーサイズリクエストコンポーネントの処理」を参照して、 が App Runner からのオーバーサイズリクエスト AWS WAF を処理する方法を確認してください。
- 適切なルールを設定しない場合、またはトラフィックパターンが変更された場合、ウェブ ACL はアプリケーションの保護にそれほど効果的ではない可能性があります。

アクセス許可

でウェブ ACL を使用するには AWS App Runner、次の IAM アクセス許可を追加します AWS WAF。

- `apprunner:ListAssociatedServicesForWebAcl`
- `apprunner:DescribeWebAclForService`
- `apprunner:AssociateWebAcl`
- `apprunner:DisassociateWebAcl`

IAM アクセス許可の詳細については、「IAM ユーザーガイド」の「IAM のポリシーとアクセス許可」を参照してください。

以下は、 の更新された IAM ポリシーの例です AWS WAF。この IAM ポリシーには、App Runner サービスを操作するために必要なアクセス許可が含まれています。

Example

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

```
            "Effect":"Allow",
            "Action":[
               "wafv2:ListResourcesForWebACL",
               "wafv2:GetWebACLForResource",
               "wafv2:AssociateWebACL",
               "wafv2:DisassociateWebACL",
               "apprunner:ListAssociatedServicesForWebAcl",
               "apprunner:DescribeWebAclForService",
               "apprunner:AssociateWebAcl",
               "apprunner:DisassociateWebAcl"
            ],
            "Resource":"*"
         }
      ]
}
```

> **Note**
>
> IAM アクセス権限を付与する必要がありますが、リストされているアクションは権限のみで、API オペレーションには対応していません。

AWS WAF ウェブ ACLs の管理

次のいずれかの方法を使用して、App Runner サービスの AWS WAF ウェブ ACLs を管理します。

- the section called “App Runner コンソール”
- the section called “AWS CLI”

App Runner コンソール

App Runner コンソールでサービスを作成したり、既存のサービスを更新したりすると、 AWS WAF ウェブ ACL の関連付けまたは関連付け解除ができます。

> **Note**
>
> - App Runner サービスは、1 つのウェブ ACL にのみ関連付けることができます。ただし、他の AWS リソースに加えて、1 つのウェブ ACL を複数の App Runner サービスに関連付けることができます。

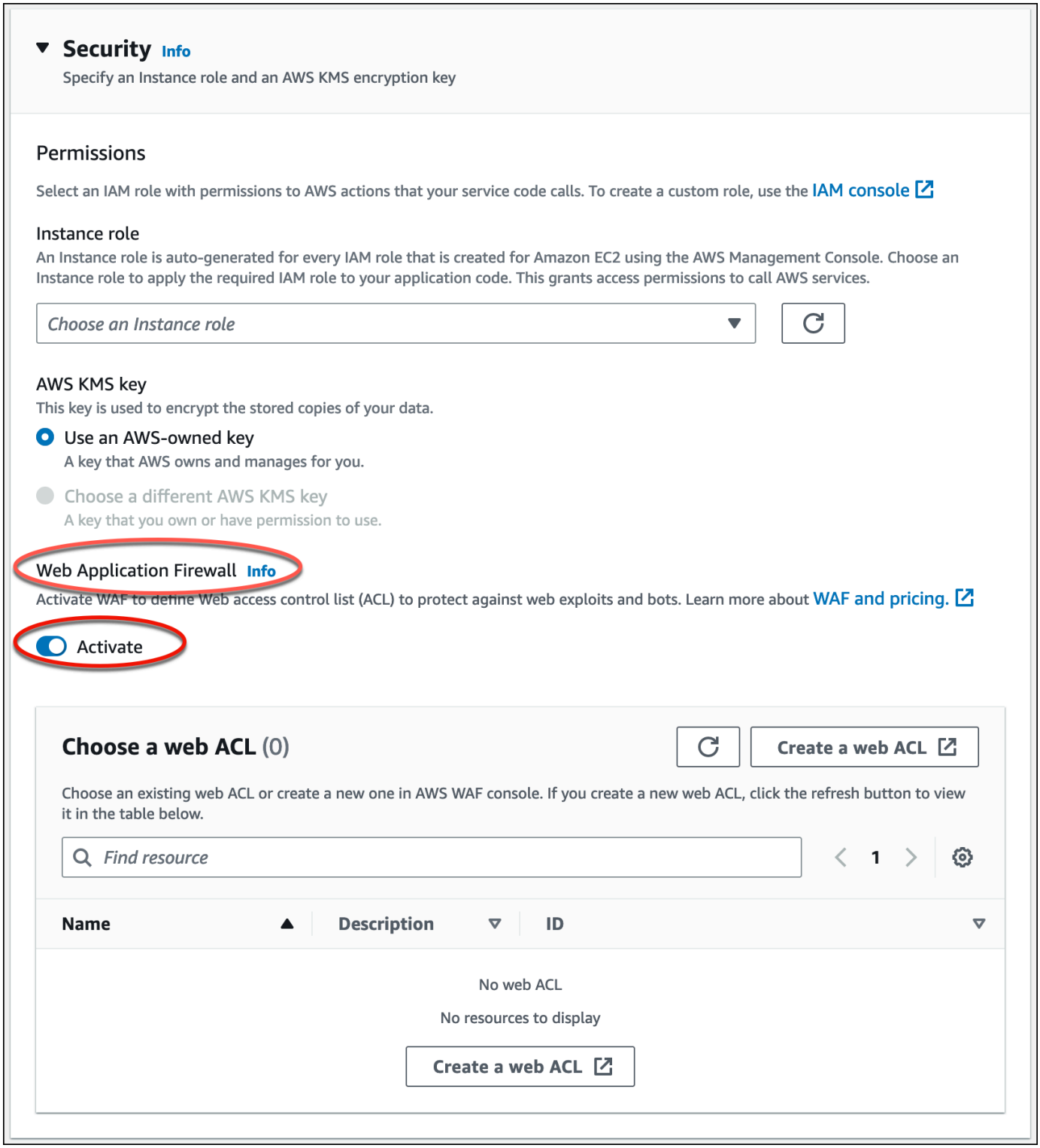
- ウェブ ACL を関連付ける前に、必ず IAM アクセス許可を更新してください AWS WAF。詳細については、「アクセス許可」を参照してください。

AWS WAF ウェブ ACL の関連付け

> **Important**
>
> WAF ウェブ ACLsルールは、IP ベースのルールに準拠していません。これは、現在、リクエストソース IP データの WAF に関連付けられた App Runner プライベートサービスへの転送をサポートしていないためです。App Runner アプリケーションにソース IP/CIDR 受信トラフィックコントロールルールが必要な場合は、WAF ウェブ ACLs の代わりにプライベートエンドポイントのセキュリティグループルールを使用する必要があります。

AWS WAF ウェブ ACL を関連付けるには

1. App Runner コンソールを開き、リージョンリストで を選択します AWS リージョン。
2. サービスを作成または更新するかどうかに基づいて、次のいずれかのステップを実行します。
   - 新しいサービスを作成する場合は、App Runner サービスの作成を選択し、サービスの設定に移動します。
   - 既存のサービスを更新する場合は、設定タブを選択し、サービスの設定で編集を選択します。
3. セキュリティでウェブアプリケーションファイアウォールに移動します。
4. トグルを有効にするボタンを選択すると、オプションが表示されます。



5. 次のいずれかのステップを実行します。

   - 既存のウェブ ACL を関連付けるには: App Runner サービスに関連付けるウェブ ACL の選択テーブルから必要なウェブ ACL を選択します。

- 新しいウェブ ACL を作成するには: AWS WAF コンソールを使用して新しいウェブ ACL を作成するには、ウェブ ACL の作成を選択します。詳細については、「デベロッパーガイド」の「ウェブ ACL の作成」を参照してください。 AWS WAF
  1. 更新ボタンを選択すると、新しく作成されたウェブ ACL がウェブ ACL の選択テーブルに表示されます。
  2. 必要なウェブ ACL を選択します。

6. 新しいサービスを作成する場合は次へ、既存のサービスを更新する場合は変更を保存するを選択します。選択したウェブ ACL は App Runner サービスに関連付けられています。
7. ウェブ ACL の関連付けを確認するには、サービスの設定タブを選択し、サービスの設定に移動します。Security の下にあるウェブアプリケーションファイアウォールにスクロールして、サービスに関連付けられたウェブ ACL の詳細を表示します。

> **Note**
>
> ウェブ ACL を作成すると、ウェブ ACL が完全に伝播され、App Runner で使用できるようになるまでに少し時間がかかります。伝達時間は数秒から数分までです。ウェブ ACL が完全に伝達される前に関連付けようとWAFUnavailableEntityExceptionすると、 は AWS WAF を返します。
> ウェブ ACL が完全に伝播される前にブラウザを更新したり、App Runner コンソールから移動したりすると、関連付けは失敗します。ただし、App Runner コンソール内を移動することはできます。

AWS WAF ウェブ ACL の関連付けを解除する

App Runner サービスを更新することで、不要になった AWS WAF ウェブ ACI の関連付けを解除できます。

AWS WAF ウェブ ACI の関連付けを解除するには

1. App Runner コンソールを開き、リージョンリストで を選択します AWS リージョン。
2. 更新するサービスの設定タブに移動し、サービスの設定で編集を選択します。
3. セキュリティでウェブアプリケーションファイアウォールに移動します。
4. トグルの有効化ボタンを無効にします。削除を確認するメッセージが表示されます。
5. [確認] を選択してください。ウェブ ACL は App Runner サービスとの関連付けが解除されます。

> **Note**
>
> - サービスを別のウェブ ACL に関連付ける場合は、ウェブ ACL の選択 テーブルからウェブ ACL を選択します。App Runner は、現在のウェブ ACL の関連付けを解除し、選択したウェブ ACL に関連付けるプロセスを開始します。
> - 関連付け解除されたウェブ ACL を使用する App Runner サービスまたはリソースが他にない場合は、ウェブ ACL の削除を検討してください。それ以外の場合は、引き続きコストが発生します。料金の詳細については、「AWS WAF 料金」を参照してください。ウェブ ACL を削除する方法については、 AWS WAF API リファレンスのDeleteWebACL」を参照してください。
> - 他のアクティブな App Runner サービスや他のリソースに関連付けられているウェブ ACL は削除できません。

AWS CLI

AWS WAF パブリック APIs を使用して、 AWS WAF ウェブ ACL の関連付けまたは関連付け解除を行うことができます。ウェブ ACL の関連付けまたは関連付け解除を行う App Runner サービスは、有効な状態である必要があります。

AWS WAF は、無効な状態の App Runner サービスに対して次のいずれか AWS WAF APIs を呼び出すと、`WAFNonexistentItemException`エラーを返します。

- `AssociateWebACL`
- `DisassociateWebACL`
- `GetWebACLForResource`

App Runner サービスの無効な状態は次のとおりです。

- `CREATE_FAILED`
- `DELETE_FAILED`
- `DELETED`
- `OPERATION_IN_PROGRESS`

> **Note**
>
> `OPERATION_IN_PROGRESS` 状態は、App Runner サービスが削除されている場合にのみ無効になります。

AWS WAF パブリック APIsAWS WAF 「 API リファレンスガイド」を参照してください。

> **Note**
>
> の IAM アクセス許可を更新します AWS WAF。詳細については、「 アクセス許可」を参照してください。

を使用した AWS WAF ウェブ ACL の関連付け AWS CLI

> **Important**
>
> WAF ウェブ ACLsルールは、IP ベースのルールに準拠していません。これは、現在、リクエストソース IP データの WAF に関連付けられた App Runner プライベートサービスへの転送をサポートしていないためです。App Runner アプリケーションにソース IP/CIDR 受信トラフィックコントロールルールが必要な場合は、WAF ウェブ ACLs の代わりにプライベートエンドポイントのセキュリティグループルールを使用する必要があります。

AWS WAF ウェブ ACL を関連付けるには

1. への優先ルールアクションのセット`Allow`またはサービスへの AWS WAF ウェブリクエストを使用して、サービスの `Block` ウェブ ACL を作成します。 AWS WAF APIs「 API AWS WAF リファレンスガイド」の「CreateWebACL」を参照してください。

   Example ウェブ ACL の作成 - リクエスト

   ```
   aws wafv2
   create-web-acl
   --region <region>
   --name <web-acl-name>
   --scope REGIONAL
   ```

```
--default-action Allow={}
--visibility-config <file-name.json>
# This is the file containing the WAF web ACL rules.
```

2. `associate-web-acl` AWS WAF パブリック API を使用して、作成したウェブ ACL を App Runner サービスに関連付けます。 AWS WAF APIs「 API AWS WAF リファレンスガイド」のAssociateWebACL」を参照してください。

> **Note**
>
> ウェブ ACL を作成すると、ウェブ ACL が完全に伝播され、App Runner で使用できるようになるまでに少し時間がかかります。伝達時間は数秒から数分までです。ウェブ ACL が完全に伝達される前に関連付けようとWAFUnavailableEntityExceptionすると、 は AWS WAF を返します。
> ウェブ ACL が完全に伝播される前にブラウザを更新したり、App Runner コンソールから移動したりすると、関連付けは失敗します。ただし、App Runner コンソール内を移動することはできます。

Example ウェブ ACL の関連付け - リクエスト

```
aws wafv2 associate-web-acl
--resource-arn <apprunner_service_arn>
--web-acl-arn <web_acl_arn>
--region <region>
```

3. `get-web-acl-for-resource` AWS WAF パブリック API を使用して、ウェブ ACL が App Runner サービスに関連付けられていることを確認します。 AWS WAF APIsAWS WAF 「 API リファレンスガイド」のGetWebACLForResource」を参照してください。

Example リソースのウェブ ACL の検証 - リクエスト

```
aws wafv2 get-web-acl-for-resource
--resource-arn <apprunner_service_arn>
--region <region>
```

サービスに関連付けられたウェブ ACLs がない場合は、空白のレスポンスが表示されます。

を使用した AWS WAF ウェブ ACL の削除 AWS CLI

App Runner サービスに関連付けられているウェブ AWS WAF ACL は削除できません。

AWS WAF ウェブ ACL を削除するには

1. `disassociate-web-acl` AWS WAF パブリック API を使用して、ウェブ ACL と App Runner サービスの関連付けを解除します。 AWS WAF APIs「 API AWS WAF リファレンスガイド」のDisassociateWebACL」を参照してください。

   Example ウェブ ACL の関連付け解除 - リクエスト

   ```
   aws wafv2 disassociate-web-acl
   --resource-arn <apprunner_service_arn>
   --region <region>
   ```

2. `get-web-acl-for-resource` AWS WAF パブリック API を使用して、ウェブ ACL と App Runner サービスの関連付けが解除されていることを確認します。

   Example ウェブ ACL の関連付けが解除されていることを確認する - リクエスト

   ```
   aws wafv2 get-web-acl-for-resource
   --resource-arn <apprunner_service_arn>
   --region <region>
   ```

   App Runner サービスに対して関連付けが解除されたウェブ ACL は表示されません。サービスに関連付けられたウェブ ACLs がない場合は、空白のレスポンスが表示されます。

3. `delete-web-acl` AWS WAF パブリック API を使用して、関連付けを解除したウェブ ACL を削除します。 AWS WAF APIs「 API AWS WAF リファレンスガイド」のDeleteWebACL」を参照してください。

   Example ウェブ ACL の削除 - リクエスト

   ```
   aws wafv2 delete-web-acl
   --name <web_acl_name>
   --scope REGIONAL
   --id <web_acl_id>
   --lock-token <web_acl_lock_token>
   --region <region>
   ```

4. `list-web-acl` AWS WAF パブリック API を使用してウェブ ACL が削除されていることを確認します。 AWS WAF APIsAWS WAF 「 API リファレンスガイド」のListWebACLs」を参照してください。

   Example ウェブ ACL が削除されたことを確認する - リクエスト

   ```
   aws wafv2 list-web-acls
   --scope REGIONAL
   --region <region>
   ```

   削除されたウェブ ACL は表示されなくなります。

   > **Note**
   > ウェブ ACL が他のアクティブな App Runner サービスまたは Amazon Cognito ユーザープールなどの他のリソースに関連付けられている場合、ウェブ ACL は削除できません。

ウェブ ACL に関連付けられている App Runner サービスの一覧表示

ウェブ ACL は、複数の App Runner サービスやその他のリソースに関連付けることができます。`list-resources-for-web-acl` AWS WAF パブリック API を使用して、ウェブ ACL に関連付けられた App Runner サービスを一覧表示します。 AWS WAF APIsAWS WAF 「 API リファレンスガイド」のListResourcesForWebACL」を参照してください。

Example ウェブ ACL に関連付けられた App Runner サービスを一覧表示する - リクエスト

```
aws wafv2 list-resources-for-web-acl
--web-acl-arn <WEB_ACL_ARN>
--resource-type APP_RUNNER_SERVICE
--region <REGION>
```

Example ウェブ ACL に関連付けられた App Runner サービスを一覧表示する - レスポンス

次の例は、ウェブ ACL に関連付けられている App Runner サービスがない場合のレスポンスを示しています。

```
{
  "ResourceArns": []
```

```
}
```

Example ウェブ ACL に関連付けられた App Runner サービスを一覧表示する - レスポンス

次の例は、ウェブ ACL に関連付けられている App Runner サービスがある場合のレスポンスを示しています。

```
{
  "ResourceArns": [
    "arn:aws:apprunner:<region>:<aws_account_id>:service/<service_name>/<service_id>"
  ]
}
```

AWS WAF ウェブ ACLsテストとログ記録

ウェブ ACL でルールアクションをカウントに設定すると、 はルールに一致するリクエストの数にリクエスト AWS WAF を追加します。App Runner サービスでウェブ ACL をテストするには、ルールアクションをカウントに設定し、各ルールに一致するリクエストの量を考慮します。例えば、通常のユーザートラフィックであると判断した多数のリクエストに一致するBlockアクションのルールを設定します。その場合は、ルールの再設定が必要になる場合があります。詳細については、「 AWS WAF デベロッパーガイド」のAWS WAF 「 保護のテストとチューニング」を参照してください。

リクエストヘッダーを Amazon CloudWatch Logs ロググループ、Amazon Simple Storage Service (Amazon S3) バケット、または Amazon Data Firehose に記録する AWS WAF ように を設定することもできます。詳細については、AWS WAF デベロッパーガイドの「ウェブ ACL トラフィックのログ記録」を参照してください。

App Runner サービスに関連付けられているウェブ ACL に関連するログにアクセスするには、次のログフィールドを参照してください。

- `httpSourceName`: を含む `APPRUNNER`
- `httpSourceId`: を含む `customeraccountid-apprunnerserviceid`

詳細については、「 AWS WAF デベロッパーガイド」の「ログの例」を参照してください。

> **Important**
>
> WAF ウェブ ACLsルールは、IP ベースのルールに準拠していません。これは、現在、リクエストソース IP データの WAF に関連付けられた App Runner プライベートサービスへの転送

をサポートしていないためです。App Runner アプリケーションにソース IP/CIDR 受信トラフィックコントロールルールが必要な場合は、WAF ウェブ ACLs の代わりにプライベートエンドポイントのセキュリティグループルールを使用する必要があります。

設定ファイルを使用した App Runner サービスオプションの設定

> **Note**
>
> 設定ファイルは、ソースコードに基づくサービスにのみ適用されます。イメージベースのサービスでは設定ファイルは使用できません。

ソースコードリポジトリを使用して AWS App Runner サービスを作成する場合、 はサービスの構築と開始に関する情報 AWS App Runner を必要とします。この情報は、App Runner コンソールまたは API を使用してサービスを作成するたびに提供できます。または、設定ファイルを使用してサービスオプションを設定することもできます。ファイルで指定するオプションはソースリポジトリの一部となり、これらのオプションへの変更は、ソースコードへの変更の追跡方法と同様に追跡されます。App Runner 設定ファイルを使用して、API がサポートするよりも多くのオプションを指定できます。API がサポートする基本オプションのみが必要な場合は、設定ファイルを提供する必要はありません。

App Runner 設定ファイルは、アプリケーションのリポジトリのソースディレクトリ`apprunner.yaml`にある という名前の YAML ファイルです。サービスのビルドとランタイムのオプションを提供します。このファイルの値は、App Runner にサービスを構築して開始する方法を指示し、ネットワーク設定や環境変数などのランタイムコンテキストを提供します。

App Runner 設定ファイルには、CPU やメモリなどのオペレーション設定は含まれていません。

App Runner 設定ファイルの例については、「」を参照してくださいthe section called “例”。完全なリファレンスガイドについては、「」を参照してくださいthe section called “参照資料”。

トピック

- App Runner 設定ファイルの例
- App Runner 設定ファイルのリファレンス

App Runner 設定ファイルの例

> **Note**
>
> 設定ファイルは、ソースコードに基づくサービスにのみ適用されます。イメージベースのサービスでは設定ファイルは使用できません。

次の例は、 AWS App Runner 設定ファイルを示しています。一部の は最小限で、必要な設定のみが含まれます。その他は、すべての設定ファイルセクションを含めて完了しています。App Runner 設定ファイルの概要については、「」を参照してくださいApp Runner 設定ファイル。

設定ファイルの例

最小設定ファイル

最小限の設定ファイルでは、App Runner は次の前提を行います。

- ビルドまたは実行中にカスタム環境変数は必要ありません。
- 最新のランタイムバージョンが使用されます。
- デフォルトのポート番号とポート環境変数が使用されます。

Example apprunner.yaml

```
version: 1.0
runtime: python3
build:
  commands:
    build:
      - pip install pipenv
      - pipenv install
run:
  command: python app.py
```

完全な設定ファイル

この例では、マネージドランタイムで`apprunner.yaml`元の形式のすべての設定キーを使用する方法を示します。

Example apprunner.yaml

```
version: 1.0
runtime: python3
build:
  commands:
    pre-build:
      - wget -c https://s3.amazonaws.com/amzn-s3-demo-bucket/test-lib.tar.gz -O - | tar
 -xz
    build:
      - pip install pipenv
      - pipenv install
    post-build:
      - python manage.py test
  env:
    - name: DJANGO_SETTINGS_MODULE
      value: "django_apprunner.settings"
    - name: MY_VAR_EXAMPLE
      value: "example"
run:
  runtime-version: 3.7.7
  command: pipenv run gunicorn django_apprunner.wsgi --log-file -
  network:
    port: 8000
    env: MY_APP_PORT
  env:
    - name: MY_VAR_EXAMPLE
      value: "example"
  secrets:
    - name: my-secret
      value-from: "arn:aws:secretsmanager:us-
east-1:123456789012:secret:testingstackAppRunnerConstr-kJFXde2ULKbT-S7t8xR:username::"
    - name: my-parameter
      value-from: "arn:aws:ssm:us-east-1:123456789012:parameter/parameter-name"
    - name: my-parameter-only-name
      value-from: "parameter-name"
```

完全な設定ファイル — (改訂されたビルドを使用)

この例では、 のすべての設定キーをマネージドランタイムapprunner.yamlで使用する方法を示します。

pre-run パラメータは、改訂された App Runner ビルドでのみサポートされます。アプリケーションが元の App Runner ビルドでサポートされているランタイムバージョンを使用している場合は、設定ファイルにこのパラメータを挿入しないでください。詳細については、「マネージドランタイムバージョンと App Runner ビルド」を参照してください。

> **Note**
>
> この例は Python 3.11 用であるため、 コマンドpip3と python3 コマンドを使用します。詳細については、Python プラットフォームトピック特定のランタイムバージョンのコールアウトの「」を参照してください。

Example apprunner.yaml

```
version: 1.0
runtime: python311
build:
  commands:
    pre-build:
      - wget -c https://s3.amazonaws.com/amzn-s3-demo-bucket/test-lib.tar.gz -O - | tar
 -xz
    build:
      - pip3 install pipenv
      - pipenv install
    post-build:
      - python3 manage.py test
  env:
    - name: DJANGO_SETTINGS_MODULE
      value: "django_apprunner.settings"
    - name: MY_VAR_EXAMPLE
      value: "example"
run:
  runtime-version: 3.11
  pre-run:
    - pip3 install pipenv
    - pipenv install
    - python3 copy-global-files.py
  command: pipenv run gunicorn django_apprunner.wsgi --log-file -
  network:
    port: 8000
    env: MY_APP_PORT
  env:
```

```
    - name: MY_VAR_EXAMPLE
      value: "example"
  secrets:
    - name: my-secret
      value-from: "arn:aws:secretsmanager:us-
east-1:123456789012:secret:testingstackAppRunnerConstr-kJFXde2ULKbT-S7t8xR:username::"
    - name: my-parameter
      value-from: "arn:aws:ssm:us-east-1:123456789012:parameter/parameter-name"
    - name: my-parameter-only-name
      value-from: "parameter-name"
```

特定のマネージドランタイム設定ファイルの例については、「」の「特定のランタイムサブトピック」を参照してください[コードベースのサービス](#)。

App Runner 設定ファイルのリファレンス

> **Note**
>
> 設定ファイルは、[ソースコードに基づくサービス](#)にのみ適用されます。[イメージベースのサービス](#)では設定ファイルは使用できません。

このトピックは、 AWS App Runner 設定ファイルの構文とセマンティクスに関する包括的なリファレンスガイドです。App Runner 設定ファイルの概要については、「」を参照してください[App Runner 設定ファイル](#)。

App Runner 設定ファイルは YAML ファイルです。に名前を付け`apprunner.yaml`、アプリケーションのリポジトリの[ソースディレクトリ](#)に配置します。

構造の概要

App Runner 設定ファイルは YAML ファイルです。に名前を付け`apprunner.yaml`、アプリケーションのリポジトリの[ソースディレクトリ](#)に配置します。

App Runner 設定ファイルには、次の主要な部分が含まれています。

- 上位セクション – 最上位キーが含まれます
- ビルドセクション – ビルドステージを設定します
- 実行セクション – ランタイムステージを設定します

上位セクション

ファイルの上部にあるキーは、ファイルとサービスランタイムに関する一般的な情報を提供します。次のキーを使用できます。

- `version` – 必須。App Runner 設定ファイルのバージョン。理想的には、最新バージョンを使用してください。

  [Syntax] (構文)

  ```
  version: version
  ```

  Example

  ```
  version: 1.0
  ```

- `runtime` – 必須。アプリケーションが使用するランタイムの名前。App Runner が提供するさまざまなプログラミングプラットフォームで使用可能なランタイムについては、「」を参照してください[コードベースのサービス](#)。

  > **Note**
  > マネージドランタイムの命名規則は *<language-name><major-version>* です。

  [Syntax] (構文)

  ```
  runtime: runtime-name
  ```

  Example

  ```
  runtime: python3
  ```

ビルドセクション

ビルドセクションでは、App Runner サービスデプロイのビルドステージを設定します。ビルドコマンドと環境変数を指定できます。ビルドコマンドが必要です。

セクションは `build:`キーで始まり、次のサブキーがあります。

- `commands` – 必須。さまざまなビルドフェーズで App Runner が実行するコマンドを指定します。次のサブキーが含まれます。
  - `pre-build` – オプション。ビルドの前に App Runner が実行するコマンド。例えば、npm依存関係をインストールしたり、ライブラリをテストしたりします。
  - `build` – 必須。App Runner がアプリケーションを構築するために実行するコマンド。例えば、を使用しますpipenv。
  - `post-build` – オプション。App Runner がビルド後に実行するコマンド。例えば、Maven を使用してビルドアーティファクトを JAR または WAR ファイルにパッケージ化するか、テストを実行します。

  [Syntax] (構文)

```
build:
  commands:
    pre-build:
      - command
      - …
    build:
      - command
      - …
    post-build:
      - command
      - …
```

  Example

```
build:
  commands:
    pre-build:
      - yum install openssl
    build:
      - pip install -r requirements.txt
    post-build:
      - python manage.py test
```

- `env` – オプション。ビルドステージのカスタム環境変数を指定します。名前と値のスカラーマッピングとして定義されます。これらの変数は、ビルドコマンドで名前で参照できます。

> **Note**
>
> この設定ファイルには、2 つの異なる場所に 2 つの異なるenvエントリがあります。1 つのセットはビルドセクションにあり、もう 1 つのセットは実行セクションにあります。
>
> - ビルドセクションの envセットは、ビルドプロセス中に pre-build、build、post-build、および pre-run コマンドで参照できます。
>
> 重要 - pre-run コマンドは、ビルドセクションで定義されている環境変数にのみアクセスできますが、このファイルの Run セクションにあることに注意してください。
> - Run セクションの envセットは、ランタイム環境の run コマンドで参照できます。

[Syntax] (構文)

```
build:
  env:
    - name: name1
      value: value1
    - name: name2
      value: value2
    - …
```

Example

```
build:
  env:
    - name: DJANGO_SETTINGS_MODULE
      value: "django_apprunner.settings"
    - name: MY_VAR_EXAMPLE
      value: "example"
```

実行セクション

実行セクションでは、App Runner アプリケーションデプロイのコンテナ実行ステージを設定します。ランタイムバージョン、実行前コマンド (変更された形式のみ) 、スタートコマンド、ネットワークポート、環境変数を指定できます。

セクションは run:キーで始まり、次のサブキーがあります。

- `runtime-version` – オプション。App Runner サービス用にロックするランタイムバージョンを指定します。

  デフォルトでは、メジャーバージョンのみがロックされます。App Runner は、デプロイまたはサービスの更新のたびにランタイムで使用できる最新のマイナーバージョンとパッチバージョンを使用します。メジャーバージョンとマイナーバージョンを指定すると、どちらもロックされ、App Runner はパッチバージョンのみを更新します。メジャーバージョン、マイナーバージョン、パッチバージョンを指定すると、サービスは特定のランタイムバージョンでロックされ、App Runner によって更新されることはありません。

  [Syntax] (構文)

  ```
  run:
    runtime-version: major[.minor[.patch]]
  ```

  > **Note**
  > 一部のプラットフォームのランタイムには、異なるバージョンコンポーネントがあります。詳細については、特定のプラットフォームのトピックを参照してください。

  Example

  ```
  runtime: python3
  run:
    runtime-version: 3.7
  ```

- `pre-run` – オプション。 ビルド使用法の改訂のみ。ビルドイメージから実行イメージにアプリケーションをコピーした後に App Runner が実行するコマンドを指定します。`/app` ディレクトリ外の実行イメージを変更するコマンドをここに入力できます。例えば、 `/app` ディレクトリの外部にある追加のグローバル依存関係をインストールする必要がある場合は、このサブセクションに必要なコマンドを入力してインストールします。App Runner ビルドプロセスの詳細については、「」を参照してくださいマネージドランタイムバージョンと App Runner ビルド。

  > **Note**
  > - 重要 — `pre-run` コマンドは実行セクションにリストされていますが、この設定ファイルのビルドセクションで定義されている環境変数のみを参照できます。この実行セクションで定義されている環境変数を参照することはできません。

- pre-run パラメータは、改訂された App Runner ビルドでのみサポートされます。アプリケーションが元の App Runner ビルドでサポートされているランタイムバージョンを使用している場合は、このパラメータを設定ファイルに挿入しないでください。詳細については、「マネージドランタイムバージョンと App Runner ビルド」を参照してください。

[Syntax] (構文)

```
run:
  pre-run:
      - command
      - …
```

- command – 必須。App Runner がアプリケーションビルドの完了後にアプリケーションを実行するために使用するコマンド。

  [Syntax] (構文)

```
run:
  command: command
```

- network – オプション。アプリケーションがリッスンするポートを指定します。この情報には以下が含まれます。
  - port – オプション。指定した場合、これはアプリケーションがリッスンするポート番号です。デフォルト: 8080。
  - env – オプション。指定した場合、App Runner はデフォルトの環境変数 で同じポート番号を渡すことに加えて (代わりに) 、この環境変数のコンテナにポート番号を渡しますPORT。つまり、 を指定するとenv、App Runner は 2 つの環境変数でポート番号を渡します。

  [Syntax] (構文)

```
run:
  network:
    port: port-number
    env: env-variable-name
```

Example

```
run:
  network:
    port: 8000
    env: MY_APP_PORT
```

- env – オプション。実行ステージのカスタム環境変数の定義。名前と値のスカラーマッピングとして定義されます。ランタイム環境では、これらの変数を名前で参照できます。

> **Note**
>
> この設定ファイルには、2 つの異なる場所に 2 つの異なるenvエントリがあります。1 つのセットはビルドセクションにあり、もう 1 つのセットは実行セクションにあります。
>
> - ビルドセクションの envセットは、ビルドプロセス中に pre-build、build、post-build、および pre-run コマンドで参照できます。
>
> 重要 - pre-run コマンドは、ビルドセクションで定義されている環境変数にのみアクセスできますが、このファイルの Run セクションにあることに注意してください。
>
> - Run セクションの envセットは、ランタイム環境の run コマンドで参照できます。

[Syntax] (構文)

```
run:
  env:
    - name: name1
      value: value1
    - name: name2
      value: value2
  secrets:
    - name: name1
      value-from: arn:aws:secretsmanager:region:aws_account_id:secret:secret-id
    - name: name2
      value-from: arn:aws:ssm:region:aws_account_id:parameter/parameter-name
    - …
```

Example

```
run:
  env:
    - name: MY_VAR_EXAMPLE
      value: "example"
  secrets:
    - name: my-secret
      value-from: "arn:aws:secretsmanager:us-
east-1:123456789012:secret:testingstackAppRunnerConstr-kJFXde2ULKbT-
S7t8xR:username::"
    - name: my-parameter
      value-from: "arn:aws:ssm:us-east-1:123456789012:parameter/parameter-name"
    - name: my-parameter-only-name
      value-from: "parameter-name"
```

App Runner API

AWS App Runner アプリケーションプログラミングインターフェイス (API) は、App Runner サービスにリクエストを行うための RESTful API です。API を使用して、 で App Runner リソースを作成、一覧表示、説明、更新、削除できます AWS アカウント。

アプリケーションコードで API を直接呼び出すことも、いずれかの AWS SDKsを使用することもできます。

API リファレンスの詳細については、AWS App Runner 「 API リファレンス」を参照してください。

デ AWS ベロッパーツールの詳細については、「構築するツール AWS」を参照してください。

トピック

- を使用して App Runner AWS CLI を操作する
- AWS CloudShell を使用して を操作する AWS App Runner

を使用して App Runner AWS CLI を操作する

コマンドラインスクリプトの場合は、 AWS CLI を使用して App Runner サービスを呼び出します。詳細な AWS CLI リファレンス情報については、AWS CLI 「 コマンドリファレンス」の「apprunner」を参照してください。

AWS CloudShell を使用すると、 AWS CLI 開発環境に をインストールせずに、 AWS Management Console 代わりに で使用できます。インストールを回避するだけでなく、認証情報を設定する必要も、リージョンを指定する必要はありません。 AWS Management Console セッションはこのコンテキストを に提供します AWS CLI。CloudShell の詳細と使用例については、「」を参照してくださいthe section called “の使用 AWS CloudShell”。

AWS CloudShell を使用して を操作する AWS App Runner

AWS CloudShell はブラウザベースの事前認証済みシェルで、 から直接起動できます AWS Management Console。任意のシェル (Bash、PowerShell、または Z シェル AWS App Runner) を使用して、 AWS サービス (を含む) に対して AWS CLI コマンドを実行できます。この手順は、コマンドラインツールのダウンロードもインストールも不要です。

AWS CloudShell から を起動 AWS Management Consoleすると、コンソールへのサインインに使用した AWS 認証情報が新しいシェルセッションで自動的に利用可能になります。 AWS CloudShell ユーザーのこの事前認証により、 AWS CLI バージョン 2 (シェルのコンピューティング環境にプリインストールされている) を使用して App Runner などの AWS サービスとやり取りするときに、認証情報の設定をスキップできます。

トピック

- の IAM アクセス許可の取得 AWS CloudShell
- を使用した App Runner の操作 AWS CloudShell
- を使用した App Runner サービスの検証 AWS CloudShell

の IAM アクセス許可の取得 AWS CloudShell

が提供するアクセス管理リソースを使用して AWS Identity and Access Management、管理者は IAM ユーザーに許可を付与し、環境の機能にアクセスして AWS CloudShell 使用できるようにします。

管理者がユーザーにアクセス権を付与する最も簡単な方法は、 AWS 管理ポリシーを使用することです。AWS マネージドポリシーは、 AWSが作成および管理するスタンドアロンポリシーです。CloudShell の次の AWS マネージドポリシーを IAM ID にアタッチできます。

- `AWSCloudShellFullAccess`: すべての機能へのフルアクセス AWS CloudShell で を使用するアクセス許可を付与します。

IAM ユーザーが実行できるアクションの範囲を制限する場合は AWS CloudShell、`AWSCloudShellFullAccess`管理ポリシーをテンプレートとして使用するカスタムポリシーを作成できます。CloudShell でユーザーが使用できるアクションの制限の詳細については、「 AWS CloudShell ユーザーガイド」の「IAM ポリシーによる AWS CloudShell アクセスと使用状況の管理」を参照してください。

> **Note**
>
> IAM ID には、App Runner を呼び出すアクセス許可を付与するポリシーも必要です。詳細については、「the section called “App Runner と IAM”」を参照してください。

を使用した App Runner の操作 AWS CloudShell

AWS CloudShell から を起動すると AWS Management Console、コマンドラインインターフェイスを使用して App Runner の操作をすぐに開始できます。

次の例では、 AWS CLI CloudShell の を使用して App Runner サービスの 1 つに関する情報を取得します。

> **Note**
>
> AWS CLI で を使用する場合 AWS CloudShell、追加のリソースをダウンロードまたはインストールする必要はありません。さらに、ユーザーはシェル内で既に認証されているので、呼び出しを行う前に認証情報を設定する必要はありません。

Example を使用した App Runner サービス情報の取得 AWS CloudShell

1. から AWS Management Console、ナビゲーションバーで使用可能な次のオプションを選択して CloudShell を起動できます。
   - CloudShell アイコンを選択します。
   - **`cloudshell`** 検索ボックスに「」と入力し始め、検索結果に CloudShell が表示されたら、そのオプションを選択します。
2. コンソールセッションの AWS リージョンにある AWS アカウント内のすべての現在の App Runner サービスを一覧表示するには、CloudShell コマンドラインで次のコマンドを入力します。

   ```
   $ aws apprunner list-services
   ```

   出力には、サービスの概要情報が一覧表示されます。

   ```
   {
     "ServiceSummaryList": [
       {
         "ServiceName": "my-app-1",
         "ServiceId": "8fe1e10304f84fd2b0df550fe98a71fa",
         "ServiceArn": "arn:aws:apprunner:us-east-2:123456789012:service/my-
   app-1/8fe1e10304f84fd2b0df550fe98a71fa",
         "ServiceUrl": "psbqam834h.us-east-1.awsapprunner.com",
   ```

```
      "CreatedAt": "2020-11-20T19:05:25Z",
      "UpdatedAt": "2020-11-23T12:41:37Z",
      "Status": "RUNNING"
    },
    {
      "ServiceName": "my-app-2",
      "ServiceId": "ab8f94cfe29a460fb8760afd2ee87555",
      "ServiceArn": "arn:aws:apprunner:us-east-2:123456789012:service/my-app-2/
ab8f94cfe29a460fb8760afd2ee87555",
      "ServiceUrl": "e2m8rrrx33.us-east-1.awsapprunner.com",
      "CreatedAt": "2020-11-06T23:15:30Z",
      "UpdatedAt": "2020-11-23T13:21:22Z",
      "Status": "RUNNING"
    }
  ]
}
```

3. 特定の App Runner サービスの詳細な説明を取得するには、前のステップで取得した ARNs のいずれかを使用して、CloudShell コマンドラインで次のコマンドを入力します。

```
$ aws apprunner describe-service --service-arn arn:aws:apprunner:us-
east-2:123456789012:service/my-app-1/8fe1e10304f84fd2b0df550fe98a71fa
```

出力には、指定したサービスの詳細な説明が一覧表示されます。

```
{
  "Service": {
    "ServiceName": "my-app-1",
    "ServiceId": "8fe1e10304f84fd2b0df550fe98a71fa",
    "ServiceArn": "arn:aws:apprunner:us-east-2:123456789012:service/my-
app-1/8fe1e10304f84fd2b0df550fe98a71fa",
    "ServiceUrl": "psbqam834h.us-east-1.awsapprunner.com",
    "CreatedAt": "2020-11-20T19:05:25Z",
    "UpdatedAt": "2020-11-23T12:41:37Z",
    "Status": "RUNNING",
    "SourceConfiguration": {
      "CodeRepository": {
        "RepositoryUrl": "https://github.com/my-account/python-hello",
        "SourceCodeVersion": {
          "Type": "BRANCH",
          "Value": "main"
        },
        "CodeConfiguration": {
```

```
          "CodeConfigurationValues": {
            "BuildCommand": "[pip install -r requirements.txt]",
            "Port": "8080",
            "Runtime": "PYTHON_3",
            "RuntimeEnvironmentVariables": [
              {
                "NAME": "Jane"
              }
            ],
            "StartCommand": "python server.py"
          },
          "ConfigurationSource": "API"
        }
      },
      "AutoDeploymentsEnabled": true,
      "AuthenticationConfiguration": {
        "ConnectionArn": "arn:aws:apprunner:us-east-2:123456789012:connection/my-
github-connection/e7656250f67242d7819feade6800f59e"
      }
    },
    "InstanceConfiguration": {
      "CPU": "1 vCPU",
      "Memory": "3 GB"
    },
    "HealthCheckConfiguration": {
      "Protocol": "TCP",
      "Path": "/",
      "Interval": 10,
      "Timeout": 5,
      "HealthyThreshold": 1,
      "UnhealthyThreshold": 5
    },
    "AutoScalingConfigurationSummary": {
      "AutoScalingConfigurationArn": "arn:aws:apprunner:us-
east-2:123456789012:autoscalingconfiguration/
DefaultConfiguration/1/00000000000000000000000000000001",
      "AutoScalingConfigurationName": "DefaultConfiguration",
      "AutoScalingConfigurationRevision": 1
    }
  }
}
```

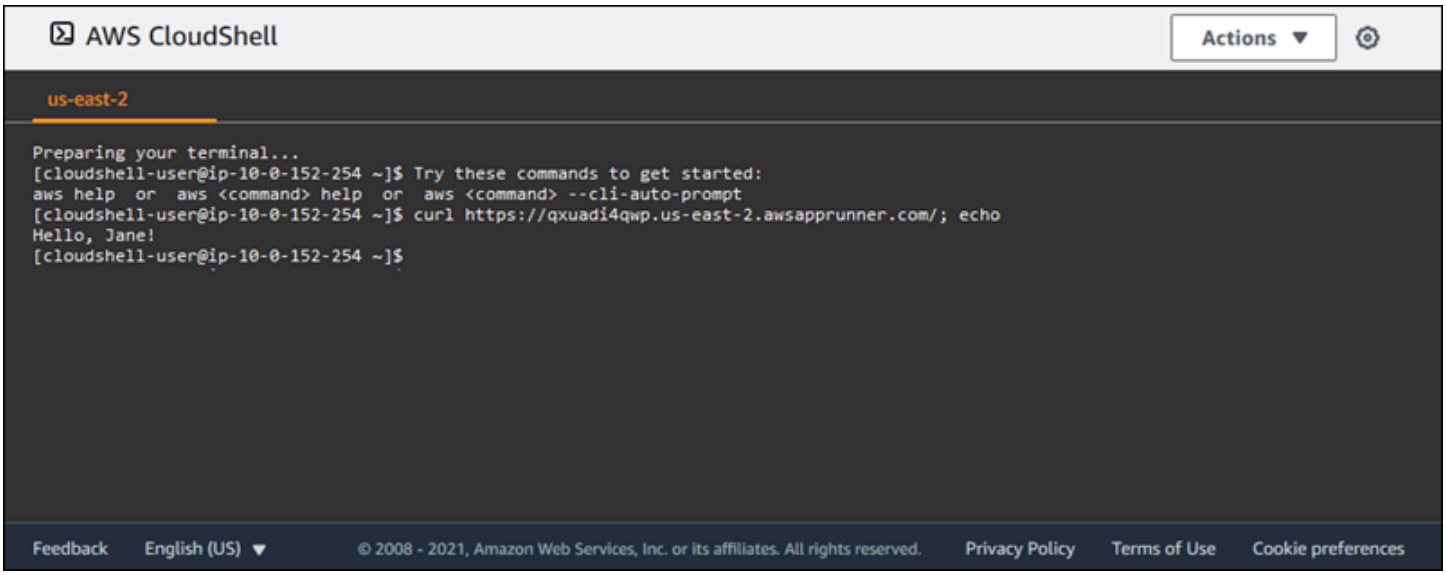
を使用した App Runner サービスの検証 AWS CloudShell

App Runner サービスを作成すると、App Runner はサービスのウェブサイトのデフォルトドメインを作成し、コンソールに表示します (または API コールの結果で返します) 。CloudShell を使用してウェブサイトを呼び出し、正しく動作していることを確認できます。

例えば、「」の説明に従って App Runner サービスを作成したら入門、CloudShell で次のコマンドを実行します。

```
$ curl https://qxuadi4qwp.us-east-2.awsapprunner.com/; echo
```

出力には、予想されるページコンテンツが表示されます。



トラブルシューティング

この章では、 AWS App Runner サービスの使用中に発生する可能性のある一般的なエラーや問題のトラブルシューティング手順について説明します。エラーメッセージは、サービスページのコンソール、API、またはログタブに表示されます。

トラブルシューティングに関するアドバイス、およびサポートへの一般的な質問に対する回答については、 ナレッジセンターにアクセスしてください。

トピック

- サービスの作成に失敗した場合
- カスタムドメイン名
- HTTP/HTTPS リクエストルーティングエラー
- サービスが Amazon RDS またはダウンストリームサービスに接続できない場合
- インスタンスの起動またはスケーリングに十分な IP アドレスがない場合

サービスの作成に失敗した場合

App Runner サービスの作成が失敗すると、サービスは `CREATE_FAILED`ステータスになります。このステータスは、コンソールで作成に失敗しましたと表示されます。以下のうち 1 つ以上に関連する問題により、サービスの作成に失敗することがあります。

- アプリケーションコード
- ビルドプロセス
- 設定
- リソースクォータ
- サービス AWS のサービス が使用する基盤となる の一時的な問題

サービスの作成に失敗した場合のトラブルシューティングを行うには、以下を実行することをお勧めします。

1. サービスイベントとログを読み、サービスの作成に失敗した原因を確認します。
2. コードまたは設定に必要な変更を加えます。

3. サービスクォータに達した場合は、1 つ以上のサービスを削除します。
4. 別のリソースクォータに達した場合は、調整可能な場合は増やすことができます。
5. 上記のすべてのステップを完了したら、もう一度サービスを再構築してみてください。サービスを再構築する方法については、「」を参照してくださいthe section called “失敗したサービスを再構築する”。

> **Note**
>
> 問題の原因となっている可能性のある調整可能なリソースクォータの 1 つは、Fargate オンデマンド vCPU リソースです。
> vCPU リソース数は、App Runner がサービスに提供できるインスタンスの数を決定します。これは、 AWS Fargate サービスに存在する Fargate オンデマンド vCPU リソース数の調整可能なクォータ値です。アカウントの vCPU クォータ設定を表示したり、クォータの引き上げをリクエストしたりするには、 の Service Quotas コンソールを使用します AWS Management Console。詳細については、「Amazon Elastic Container Service デベロッパーガイド」の「Service AWS Fargate Quotas」を参照してください。

> **Important**
>
> 失敗したサービスの最初の作成試行以降に追加料金は発生しません。失敗したサービスは使用できませんが、サービスクォータにカウントされます。App Runner は、失敗したサービスを自動的に削除しないため、障害の分析が終了したら削除してください。

カスタムドメイン名

このセクションでは、カスタムドメインにリンクするときに発生する可能性のあるさまざまなエラーをトラブルシューティングして解決する方法について説明します。

> **Note**
>
> App Runner アプリケーションのセキュリティを強化するために、*.awsapprunner.com ドメインはパブリックサフィックスリスト (PSL) に登録されています。セキュリティを強化するために、App Runner アプリケーションのデフォルトドメイン名に機密 Cookie を設定する必要がある場合は、`__Host-`プレフィックス付きの Cookie を使用することをお勧めします。このプラクティスは、クロスサイトリクエストフォージェリ (CSRF) 攻撃からドメインを防

ぐ際に役立ちます。詳細については、Mozilla 開発者ネットワークの「Set-Cookie」ページを参照してください。

カスタムドメインの作成失敗エラーの取得

- このエラーが CAA レコードの問題によるものであるかどうかを確認します。DNS ツリーのどこに CAA レコードがない場合、メッセージ を受け取りfail open、カスタムドメインを検証するための証明書 AWS Certificate Manager を発行します。これにより、App Runner はカスタムドメインを受け入れることができます。DNS レコードで CAA 証明書を使用している場合は、少なくとも 1 つのドメインの CAA レコードに が含まれていることを確認してくださいamazon.com。それ以外の場合、ACM は証明書の発行に失敗します。その結果、App Runner のカスタムドメインは作成されません。

  次の例では、DNS ルックアップツール DiG を使用して、必要なエントリが欠落している CAA レコードを表示します。この例では、 をカスタムドメインexample.comとして使用します。この例で次のコマンドを実行して、CAA レコードを確認します。

  ```
  ...
  ;; QUESTION SECTION:
  ;example.com.           IN  CAA

  ;; ANSWER SECTION:
  example.com.        7200    IN  CAA 0 iodef "mailto:hostmaster@example.com"
  example.com.        7200    IN  CAA 0 issue "letsencrypt.org"
  ...note absence of "amazon.com" in any of the above CAA records...
  ```

- ドメインレコードを修正し、少なくとも 1 つの CAA レコードに が含まれていることを確認しますamazon.com。
- カスタムドメインと App Runner のリンクを再試行してください。

CAA エラーを解決する方法については、以下を参照してください。

- 認証機関認可 (CAA) の問題
- ACM 証明書の発行または更新に関する CAA エラーを解決するにはどうすればよいですか？

カスタムドメインの DNS 証明書検証保留中エラーの取得

- カスタムドメイン設定の重要なステップをスキップしたかどうかを確認します。さらに、DiG などの DNS ルックアップツールを使用して DNS レコードを誤って設定していないかも確認します。特に、次の間違いがないか確認します。
  - 見逃したステップ。
  - DNS レコードの二重引用符などのサポートされていない文字。
- 間違いを修正します。
- カスタムドメインと App Runner のリンクを再試行してください。

CAA 検証エラーを解決する方法については、以下を参照してください。

- DNS 検証
- the section called “カスタムドメイン名”

基本的なトラブルシューティングコマンド

- サービスが見つかったことを確認します。

```
aws apprunner list-services
```

- サービスを記述し、そのステータスを確認します。

```
aws apprunner describe-service --service-arn
```

- カスタムドメインのステータスを確認します。

```
aws apprunner describe-custom-domains --service-arn
```

- 進行中のすべてのオペレーションを一覧表示します。

```
aws apprunner list-operations --service-arn
```

カスタムドメイン証明書の更新

サービスにカスタムドメインを追加すると、App Runner は DNS サーバーに追加する一連の CNAME レコードを提供します。これらの CNAME レコードには、証明書レコードが含まれます。App Runner は AWS Certificate Manager (ACM) を使用してドメインを検証します。App Runner は、これらの DNS レコードを検証して、このドメインの所有権が継続していることを確認します。DNS ゾーンから CNAME レコードを削除すると、App Runner は DNS レコードを検証できなくなり、カスタムドメイン証明書は自動的に更新されません。

このセクションでは、次のカスタムドメイン証明書の更新の問題を解決する方法について説明します。

- the section called “CNAME が DNS サーバーから削除されます”.
- the section called “証明書の有効期限が切れています”.

CNAME が DNS サーバーから削除されます

- DescribeCustomDomains API を使用するか、App Runner コンソールのカスタムドメイン設定から CNAME レコードを取得します。保存された CNAMEs「 CertificateValidationRecords」を参照してください。
- 証明書検証 CNAME レコードを DNS サーバーに追加します。App Runner は、ドメインを所有していることを検証できます。CNAME レコードを追加した後、DNS レコードが伝播されるまでに最大 30 分かかることがあります。App Runner と ACM が証明書の更新プロセスを再試行するまでに数時間かかることもあります。CNAME レコードを追加する方法については、「」を参照してくださいthe section called “カスタムドメインの管理”。

証明書の有効期限が切れています

- App Runner コンソールまたは API を使用して、App Runner サービスのカスタムドメインの関連付けを解除 (リンク解除) してから、関連付け (リンク) します。App Runner は、新しい証明書検証 CNAME レコードを作成します。
- 新しい証明書検証 CNAME レコードを DNS サーバーに追加します。

カスタムドメインの関連付けを解除 (リンク解除) および関連付け (リンク) する方法については、「」を参照してくださいthe section called “カスタムドメインの管理”。

証明書が正常に更新されたことを確認する方法

証明書レコードのステータスを確認して、証明書が正常に更新されたことを確認できます。curl などのツールを使用して、証明書のステータスを確認できます。

証明書の更新の詳細については、次のリンクを参照してください。

- ACM 証明書が更新対象外としてマークされるのはなぜですか？
- ACM 証明書のマネージド更新
- DNS 検証

HTTP/HTTPS リクエストルーティングエラー

このセクションでは、App Runner サービスエンドポイントに HTTP/HTTPS トラフィックをルーティングするときに発生する可能性のあるエラーをトラブルシューティングして解決する方法について説明します。

404 App Runner サービスエンドポイントに HTTP/HTTPS トラフィックを送信するときにエラーが見つからない

- App Runner `Host Header`がホストヘッダー情報を使用してリクエストをルーティングするため、 が HTTP リクエストのサービス URL を指していることを確認します。cURL、、ウェブブラウザなどのほとんどのクライアントは、ホストヘッダーを自動的にサービス URL にポイントします。クライアントがサービス URL を として設定しない場合`Host Header`、`404 Not Found`エラーが発生します。

  Example ホストヘッダーが正しくない

  ```
  $ ~ curl -I -H "host: foobar.com" https://testservice.awsapprunner.com/
  HTTP/1.1 404 Not Found
  transfer-encoding: chunked
  ```

Example 正しいホストヘッダー

```
$ ~ curl -I -H "host: testservice.awsapprunner.com" https://
testservice.awsapprunner.com/
HTTP/1.1 200 OK
content-length: 11772
content-type: text/html; charset=utf-8
```

- クライアントがパブリックサービスまたはプライベートサービスへのリクエストルーティング用にサーバー名インジケータ (SNI) を正しく設定していることを確認します。TLS の終了とリクエストのルーティングの場合、App Runner は HTTPS 接続で設定された SNI を使用します。

サービスが Amazon RDS またはダウンストリームサービスに接続できない場合

Amazon RDS データベースや他のダウンストリームアプリケーションやサービスへの接続に失敗すると、サービスにネットワーク設定の問題が発生する可能性があります。このトピックでは、ネットワーク設定に問題があるかどうかを判断する手順と、それらを修正するオプションについて説明します。App Runner のアウトバウンドトラフィック設定の詳細については、「」を参照してください送信トラフィックの VPC アクセスの有効化 。

> **Note**
>
> VPC Connector の設定を表示するには、App Runner コンソールの左側のナビゲーションペインから、ネットワーク設定を選択します。次に、送信トラフィックタブを選択します。VPC コネクタを選択します。次のページには、VPC コネクタの詳細が表示されます。このページでは、VPC を使用するサブネット、セキュリティグループ、App Runner サービスを表示およびドリルダウンできます。

アプリケーションが別のダウンストリームサービスに接続できない原因を絞り込むには

1. VPC コネクタで使用されるサブネットがプライベートサブネットであることを確認します。コネクタがパブリックサブネットで設定されている場合、各サブネットの基盤となる Hyperplane ENIs (Elastic Network Interface) にパブリック IP スペースがないため、サービスでエラーが発生します。

VPC コネクタがパブリックサブネットを使用している場合は、この設定を修正するための以下のオプションがあります。

a. 新しいプライベートサブネットを作成し、VPC Connector のパブリックサブネットの代わりに使用します。詳細については、「Amazon VPC ユーザーガイド」の「VPC のサブネット」を参照してください。

b. 既存のパブリックサブネットを NAT ゲートウェイ経由でルーティングします。詳細については、「Amazon VPC ユーザーガイド」の「NAT ゲートウェイ」を参照してください。

2. VPC Connector のセキュリティグループの入出力ルールが正しいことを確認します。App Runner コンソールの左側のナビゲーションペインから、ネットワーク設定 > 送信トラフィックを選択します。リストから VPC コネクタを選択します。次のページには、検査するために選択できるセキュリティグループが一覧表示されます。

3. 接続しようとしている RDS インスタンスまたはその他のダウンストリームサービスに対して、セキュリティグループのインバウンドルールとアウトバウンドルールが正しいことを確認します。詳細については、App Runner アプリケーションが接続しようとしているダウンストリームサービスのサービスガイドを参照してください。

4. App Runner 設定の外部で他のタイプのネットワーク設定の問題がないことを確認するには、App Runner の外部で RDS またはダウンストリームサービスに接続してみてください。

   a. 同じ VPC 内の Amazon EC2 インスタンスから、RDS インスタンスまたはサービスに接続してみてください。

   b. サービス VPC エンドポイントに接続しようとしている場合は、同じ VPC 内の EC2 インスタンスから同じエンドポイントにアクセスして接続を確認します。

5. ステップ 4 の接続テストのいずれかが失敗した場合、App Runner 設定の外部で AWSアカウント内の別のリソースに問題がある可能性があります。 AWS サポートに連絡して、他のネットワーク設定の問題をさらに分離して修正してください。

6. ステップ 4 の手順を実行して RDS インスタンスまたはダウンストリームサービスに正常に接続する場合は、このステップの手順に進みます。Hyperplane ENI フローログを有効にして検査することで、トラフィックが ENI に入り込んでいるかどうかを確認します。

> **Note**
>
> これらのステップを完了して必要な ENI フローログ情報を取得するには、App Runner サービスが正常に起動した後に RDS またはダウンストリームサービスへの接続試行を行う必要があります。アプリケーションは、実行中状態のときに RDS またはダウンス

トリームサービスへの接続オペレーションを実行する必要があります。それ以外の場合、ENIsは App Runner のロールバックワークフローの一部としてクリーンアップできます。このアプローチにより、ENIsを引き続き詳細に調査できます。

a. AWS コンソールから EC2 コンソールを起動します。

b. 左側のナビゲーションペインのネットワークとセキュリティのグループで、ネットワークインターフェイスを選択します。

c. インターフェイスタイプ列と説明列にスクロールして、VPC コネクタに関連付けられたサブネット内の ENIs を見つけます。次の命名パターンがあります。

   - インターフェイスタイプ： Fargate
   - 説明: で始まる AWSAppRunner ENI (例: AWSAppRunner ENI - abcde123-abcd-1234-1234-abcde1233456)

d. 行の先頭にあるチェックボックスを使用して、適用する ENIsを選択します。

e. アクションメニューからフローログの作成を選択します。

f. プロンプトに情報を入力し、ページの下部にあるフローログの作成を選択します。

g. 生成されたフローログを検査します。

   - 接続のテスト中にトラフィックが ENI に入り込んでいた場合、問題は ENI のセットアップとは関係ありません。App Runner サービス以外の AWS アカウント内の別のリソースでネットワーク設定の問題が発生する可能性があります。詳細については、 サポートにお問い合わせください AWS 。
   - 接続のテスト中にトラフィックが ENI に入らなかった場合は、 AWS サポートに連絡して、Fargate サービスに既知の問題があるかどうか確認することをお勧めします。

h. ネットワーク Reachability Analyzer ツールを使用します。このツールは、仮想ネットワークパスのソースに到達できない場合にブロックコンポーネントを特定することで、ネットワークの設定ミスを判断するのに役立ちます。詳細については、「Amazon VPC Reachability Analyzer ガイド」の「Reachability Analyzer とは」を参照してください。

   App Runner ENI をソースとして、RDS ENI を送信先として入力します。

7. 問題をさらに絞り込むことができない場合、または前のステップを完了した後も RDS またはダウンストリームサービスに接続できない場合は、 AWS サポートに連絡してサポートを受けることをお勧めします。

インスタンスの起動またはスケーリングに十分な IP アドレスがない場合

> **Note**
>
> パブリックサービスの場合、App Runner は VPCs に Elastic Network Interface (ENI) を作成しないため、パブリックサービスはこの変更の影響を受けません。

このガイドは、送信トラフィックの VPC アクセスが有効になっている App Runner サービスで発生する可能性のある IP 枯渇エラーを解決するのに役立ちます。

App Runner は、VPC コネクタに関連付けられたサブネットでインスタンスを起動します。App Runner は、インスタンスが起動されるサブネットにインスタンスごとに 1 つの ENI を作成します。各 ENI は、そのサブネットでプライベート IP を使用します。サブネットには、そのサブネットに関連付けられた CIDR ブロックに応じて、使用可能な IPs の数は一定です。App Runner が ENI を作成するのに十分な IPs を持つサブネット (複数可) を見つけることができない場合、App Runner サービスの新しいインスタンスを起動できません。これにより、サービスのスケールアップに関する問題が発生する可能性があります。このような場合、App Runner イベントログが表示され、App Runner が使用可能な IPs を持つサブネットを見つけることができないことが示されます。このようなエラーを解決するには、以下の手順でサービスを更新できます。

サービスを更新して利用可能な IPsを増やす方法

サブネットで使用可能な IP アドレスの数は、そのサブネットに関連付けられた CIDR ブロックに基づきます。サブネットに関連付けられた CIDR ブロックは、作成後に更新することはできません。App Runner VPC コネクタは、作成後に更新することもできません。App Runner サービスにさらに多くの IPs を提供するには、送信トラフィックを有効にするための VPC アクセスを有効にします。

1. CIDR ブロックが大きい新しいサブネット (複数可) を作成します。
2. 新しいサブネット (複数可) を使用して新しい VPC コネクタを作成します。
3. 新しい VPC コネクタを使用するように App Runner サービスを更新します。

サービスに必要な IPsの計算

より大きな CIDR ブロックを使用して新しいサブネット (複数可) を作成する前に、App Runner サービス全体で必要な IPs の数を決定します。コネクタに必要な IPs の数は、次のように計算することをお勧めします。

1. 送信トラフィックに対する VPC アクセスが有効になっているサービスごとに、自動スケーリング設定の最大サイズ (最大インスタンス) を書き留めます。
2. すべてのサービスで値を合計します。
3. Blue-Green デプロイ中に起動される新しいインスタンスを考慮して、この合計を 2 倍にします。

例

同じ VPC コネクタを使用する 2 つのサービス A と B について考えてみましょう。

1. サービス A の最大サイズは 25 に設定されています。
2. サービス B の最大サイズは 15 に設定されています。

必要な IPs = 2 × (25 + 15) = 80

サブネットに少なくとも 80 個の使用可能な IPsが組み合わされていることを確認します。

新しいサブネットを作成する (複数可)

1. この式を使用して、IPv4 に必要な CIDR ブロックサイズを決定します (5 つの IPs は AWS: サブネットのサイズ設定によって予約されていることに注意してください)。

```
Number of available IP addresses = 2^(32 - prefix length) - 5
```

```
Example :
For 192.168.1.0/24:
Prefix length is 24
Number of available IP addresses = 2^(32 - 24) - 5 = 2^8-5 = 251 IP addresses

For 10.0.0.0/16:
Prefix length is 16
Number of available IP addresses = 2^(32 - 16) - 5 = 2^16-5 = 65,531 IP addresses
```

```
Quick reference:
/24 = 251 IP addresses
/16 = 65,531 IP addresses
```

2. AWS EC2 CLI を使用して新しいサブネットを作成します。

```
aws ec2 create-subnet --vpc-id <my-vpc-id> --cidr-block <cidr-block>
```

例 (4,096 IPs を持つサブネットを作成)

```
aws ec2 create-subnet --vpc-id my-vpc-id --cidr-block 10.0.0.0/20
```

3. 新しい VPC コネクタを作成します。「」を参照: VPC アクセスを管理する
4. この新しい VPC コネクタを使用するように VPC への送信トラフィックを有効にしてサービスを更新します。サービスが更新されると、App Runner は新しいサブネットの使用を開始します。

> **Note**
>
> VPCsは、CIDR ブロックによってサブネットに割り当てることができる使用可能な IPs の数にも制限されます。CIDR ブロックが大きいサブネットを作成できない場合は、新しいサブネット (複数可) を作成する前に VPC をセカンダリ CIDR ブロックで更新する必要がある場合があります。

VPC へのセカンダリ CIDR ブロックのアタッチ

セカンダリ CIDR ブロックをこの VPC に関連付けます。

```
aws ec2 associate-vpc-cidr-block --vpc-id <my-vpc-id> --cidr-block <cidr-block>
```

例 :

```
aws ec2 associate-vpc-cidr-block --vpc-id my-vpc-id --cidr-block 10.1.0.0/16
```

検証

サービスを更新したら、以下を使用して、修正の検証を実行できます。

1. イベントログをモニタリングする: App Runner サービスイベントログをモニタリングして、新しい IP または ENI 利用不能エラーが表示されないことを確認します。
2. Service Scaling を確認します。
    1. 自動スケーリング設定で最小インスタンス数を変更してサービスを完全にスケールアップする
    2. IP 関連のエラーなしですべての新しいインスタンスが起動されることを確認する
    3. 複数のスケーリングイベントをモニタリングして、一貫したパフォーマンスを確保する
3. コンソールバナー: AWS マネジメントコンソールを使用している場合は、App Runner が IPs 不足に関するバナー警告を表示しなくなったことを確認します。
4. VPC とサブネット IP 使用率:
    1. VPC ダッシュボードまたは CLI コマンドを使用して、新しいサブネットの IP アドレス使用率を確認します。
    2. サービスのスケールアップ後も使用可能な IPs のマージンが正常であることを確認する

一般的な落とし穴

App Runner サービスで IP の枯渇に対処するときは、以下の潜在的な問題に注意してください。

1. IP アドレスの計画が不十分: 将来の IP ニーズを過小評価すると、枯渇の問題が繰り返し発生する可能性があります。潜在的なサービスの増加とピーク使用シナリオを考慮して、徹底的なキャパシティプランニングを実施します。
2. VPC 全体の IP 使用状況を見落としている： 同じ VPC 内の他の AWS のサービスも IP アドレスを消費することに注意してください。VPC とサブネットの設定を計画するときは、すべてのサービスの IP 要件を考慮してください。
3. サービスの更新を無視する: 新しいサブネットまたは VPC コネクタを作成したら、新しい設定を使用するように App Runner サービスを更新してください。そうしないと、使い果たされた IP 範囲が引き続き使用されます。
4. CIDR ブロックの重複の誤解： VPC にセカンダリ CIDR ブロックを追加するときは、既存のブロックと重複しないようにしてください。CIDR ブロックが重複すると、ルーティングの競合や IP アドレスのあいまいさが発生する可能性があります。

5. VPC の制限の超過: VPC は最大 5 つの CIDR ブロック (1 つのプライマリと 4 つのセカンダリ) を持つことができることに注意してください。これらの制約内で IP アドレス空間の拡張を計画します。
6. サブネット AZ ディストリビューションを無視する: 新しいサブネットを作成するときは、高可用性と耐障害性を確保するために、複数のアベイラビリティーゾーンに分散されていることを確認します。
7. ENI の制限を見落としている: インスタンスにアタッチできる ENIs の数には制限があることに注意してください。AWS アカウントの制限が、計画されたネットワークインターフェイスの使用と一致していることを確認します。

これらの落とし穴を認識することで、VPC リソースをより効果的に管理し、App Runner サービスの IP 枯渇の問題を回避できます。

その他のリソース

1. AWS VPC ドキュメント
2. CIDR ブロックについて
3. App Runner VPC コネクタ

用語集

1. ENI:Elastic Network Interface、AWS の仮想ネットワークインターフェイス。
2. CIDR:Classless Inter-Domain Routing、IP アドレスを割り当てる方法。
3. VPC コネクタ: App Runner が VPC に接続できるようにするリソース。

App Runner のセキュリティ

でのクラウドセキュリティが最優先事項 AWS です。 AWS のお客様は、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からメリットを得られます。

セキュリティは、 AWS とお客様の間で共有される責任です。責任共有モデルでは、これをクラウドのセキュリティおよびクラウド内のセキュリティと説明しています。

- クラウドのセキュリティ – AWS は、 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責任があります AWS クラウド。 AWS また、 は、お客様が安全に使用できるサービスも提供します。コンプライアンスAWS プログラムコンプライアンス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者は定期的にセキュリティの有効性をテストおよび検証。が適用されるコンプライアンスプログラムの詳細については AWS App Runner、「コンプライアンスプログラムAWS による対象範囲内のサービスコンプライアンスプログラム」を参照してください。
- クラウド内のセキュリティ – お客様の責任は、使用する AWS サービスによって決まります。また、ユーザーは、データの機密性、会社の要件、適用される法律や規制など、その他の要因についても責任を負います。

このドキュメントは、App Runner を使用する際の責任共有モデルの適用方法を理解するのに役立ちます。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ように App Runner を設定する方法について説明します。また、App Runner リソースのモニタリングや保護に役立つ他の AWS サービスの使用方法についても説明します。

トピック

- App Runner でのデータ保護
- App Runner の Identity and Access Management
- App Runner でのログ記録とモニタリング
- App Runner のコンプライアンス検証
- App Runner の耐障害性
- のインフラストラクチャセキュリティ AWS App Runner
- VPC エンドポイントでの App Runner の使用
- App Runner での設定と脆弱性の分析
- App Runner のセキュリティのベストプラクティス

App Runner でのデータ保護

責任 AWS 共有モデル、 でのデータ保護に適用されます AWS App Runner。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 Identity Center 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、その中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 App Runner 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。

その他の App Runner セキュリティトピックについては、「」を参照してくださいセキュリティ。

トピック

- 暗号化を使用したデータの保護
- インターネットトラフィックのプライバシー

暗号化を使用したデータの保護

AWS App Runner は、指定したリポジトリからアプリケーションソース (ソースイメージまたはソースコード) を読み取り、サービスにデプロイするために保存します。詳細については、「アーキテクチャと概念」を参照してください。

データ保護とは、転送中 (App Runner との間でデータを送受信するとき) および保管中 (AWS データセンターに格納されているとき) のデータを保護することです。

データ保護の詳細については、「the section called “データ保護”」を参照してください。

その他の App Runner セキュリティトピックについては、「」を参照してくださいセキュリティ。

転送中の暗号化

転送中のデータ保護は、Transport Layer Security (TLS) を使用して接続を暗号化するか、クライアント側の暗号化 (オブジェクトが送信される前に暗号化される) を使用するという 2 つの方法で実現できます。どちらの方法も、アプリケーションデータを保護するために有効です。接続を保護するには、アプリケーション、開発者、管理者、エンドユーザーがオブジェクトを送受信するたびに、TLS を使用して暗号化します。App Runner は、TLS 経由でトラフィックを受信するようにアプリケーションを設定します。

クライアント側の暗号化は、デプロイのために App Runner に提供するソースイメージまたはコードを保護する有効な方法ではありません。App Runner はアプリケーションソースにアクセスする必要があるため、暗号化できません。したがって、開発環境またはデプロイ環境と App Runner 間の接続は必ず保護してください。

保管時の暗号化とキー管理

保管中のアプリケーションのデータを保護するために、App Runner はアプリケーションソースイメージまたはソースバンドルの保存されたすべてのコピーを暗号化します。App Runner サービスを作成するときに、 を指定できます AWS KMS key。指定した場合、App Runner は指定されたキーを使用してソースを暗号化します。指定しない場合、App Runner は AWS マネージドキー 代わりに を使用します。

App Runner サービス作成パラメータの詳細については、CreateService」を参照してください。AWS Key Management Service（AWS KMS) の詳細については、「AWS Key Management Service デベロッパーガイド」を参照してください。

インターネットトラフィックのプライバシー

App Runner はAmazon Virtual Private Cloud (Amazon VPC) を使用して、App Runner アプリケーションのリソース間に境界を作成し、リソース、オンプレミスネットワーク、インターネット間のトラフィックを制御します。Amazon VPC セキュリティの詳細については、「Amazon VPC ユーザーガイド」の「Amazon VPC でのインターネットワークトラフィックのプライバシー」を参照してください。

App Runner アプリケーションをカスタム Amazon VPC に関連付ける方法については、「」を参照してくださいthe section called “送信トラフィック”。

VPC エンドポイントを使用して App Runner へのリクエストを保護する方法については、「」を参照してくださいthe section called “VPC エンドポイント”。

データ保護の詳細については、「the section called “データ保護”」を参照してください。

その他の App Runner セキュリティトピックについては、「」を参照してくださいセキュリティ。

App Runner 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 App Runner リソースの使用を承認する (アクセス許可を付与する) かを制御します。IAM は、追加料金なしで AWS のサービス 使用できる です。

その他の App Runner セキュリティトピックについては、「」を参照してくださいセキュリティ。

トピック

- 対象者
- 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
- App Runner と IAM の連携方法
- App Runner アイデンティティベースのポリシーの例
- App Runner のサービスにリンクされたロールの使用

- AWS の マネージドポリシー AWS App Runner
- App Runner 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

対象者

AWS Identity and Access Management (IAM) の使用方法は、App Runner で行う作業によって異なります。

サービスユーザー – App Runner サービスを使用してジョブを実行する場合、管理者から必要な認証情報とアクセス許可が与えられます。さらに多くの App Runner 機能を使用して作業を行う場合は、追加のアクセス許可が必要になることがあります。アクセスの管理方法を理解すると、管理者に適切なアクセス許可をリクエストするのに役に立ちます。App Runner の機能にアクセスできない場合は、「」を参照してくださいApp Runner 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。

サービス管理者 – 社内の App Runner リソースを担当している場合は、通常、App Runner へのフルアクセスがあります。サービスユーザーがどの App Runner 機能やリソースにアクセスするかを決めるのは管理者の仕事です。その後、IAM 管理者にリクエストを送信して、サービスユーザーの権限を変更する必要があります。このページの情報を点検して、IAM の基本概念を理解してください。会社で App Runner で IAM を使用する方法の詳細については、「」を参照してくださいApp Runner と IAM の連携方法。

IAM 管理者 – IAM 管理者は、App Runner へのアクセスを管理するポリシーの作成方法の詳細について確認する場合があります。IAM で使用できる App Runner 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App Runner アイデンティティベースのポリシーの例。

アイデンティティを使用した認証

認証とは、ID 認証情報 AWS を使用して にサインインする方法です。として、IAM ユーザーとして AWS アカウントのルートユーザー、または IAM ロールを引き受けて認証 (サインイン AWS) される必要があります。

ID ソースを介して提供された認証情報を使用して、フェデレーティッド ID AWS として にサインインできます。 AWS IAM Identity Center（ IAM Identity Center) ユーザー、会社のシングルサインオン認証、Google または Facebook 認証情報は、フェデレーティッド ID の例です。フェデレーティッド ID としてサインインする場合、IAM ロールを使用して、前もって管理者により ID フェデレーションが設定されています。フェデレーション AWS を使用して にアクセスすると、間接的にロールを引き受けることになります。

ユーザーのタイプに応じて、 AWS Management Console または AWS アクセスポータルにサインインできます。へのサインインの詳細については AWS、「 AWS サインイン ユーザーガイド」の「 にサインインする方法 AWS アカウント」を参照してください。

AWS プログラムで にアクセスする場合、 は Software Development Kit (SDK) とコマンドラインインターフェイス (CLI) AWS を提供し、認証情報を使用してリクエストに暗号で署名します。 AWS ツールを使用しない場合は、リクエストに自分で署名する必要があります。リクエストに自分で署名する推奨方法の使用については、「IAM ユーザーガイド」の「API リクエストに対するAWS Signature Version 4」を参照してください。

使用する認証方法を問わず、追加セキュリティ情報の提供をリクエストされる場合もあります。例えば、 では、アカウントのセキュリティを強化するために多要素認証 (MFA) を使用する AWS ことをお勧めします。詳細については、「AWS IAM Identity Center ユーザーガイド」の「多要素認証」および「IAM ユーザーガイド」の「IAM のAWS 多要素認証」を参照してください。

AWS アカウント ルートユーザー

を作成するときは AWS アカウント、アカウント内のすべての およびリソースへの AWS のサービス完全なアクセス権を持つ 1 つのサインインアイデンティティから始めます。この ID は AWS アカウント ルートユーザーと呼ばれ、アカウントの作成に使用した E メールアドレスとパスワードでサインインすることでアクセスできます。日常的なタスクには、ルートユーザーを使用しないことを強くお勧めします。ルートユーザーの認証情報は保護し、ルートユーザーでしか実行できないタスクを実行するときに使用します。ルートユーザーとしてサインインする必要があるタスクの完全なリストについては、IAM ユーザーガイドの「ルートユーザー認証情報が必要なタスク」を参照してください。

IAM ユーザーとグループ

IAM ユーザーは、1 人のユーザーまたはアプリケーションに対して特定のアクセス許可 AWS アカウント を持つ 内のアイデンティティです。可能であれば、パスワードやアクセスキーなどの長期的な認証情報を保有する IAM ユーザーを作成する代わりに、一時的な認証情報を使用することをお勧めします。ただし、IAM ユーザーでの長期的な認証情報が必要な特定のユースケースがある場合は、アクセスキーをローテーションすることをお勧めします。詳細については、「IAM ユーザーガイド」の「長期的な認証情報を必要とするユースケースのためにアクセスキーを定期的にローテーションする」を参照してください。

IAM グループは、IAM ユーザーの集団を指定するアイデンティティです。グループとしてサインインすることはできません。グループを使用して、複数のユーザーに対して一度に権限を指定できます。多数のユーザーグループがある場合、グループを使用することで権限の管理が容易になります。

例えば、IAMAdmins という名前のグループを設定して、そのグループに IAM リソースを管理する許可を与えることができます。

ユーザーは、ロールとは異なります。ユーザーは 1 人の人または 1 つのアプリケーションに一意に関連付けられますが、ロールはそれを必要とする任意の人が引き受けるようになっています。ユーザーには永続的な長期の認証情報がありますが、ロールでは一時認証情報が提供されます。詳細については、「IAM ユーザーガイド」の「IAM ユーザー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 AWS アカウント を持つ 内のアイデンティティです。これは IAM ユーザーに似ていますが、特定のユーザーには関連付けられていません。で IAM ロールを一時的に引き受けるには AWS Management Console、ユーザーから IAM ロール (コンソール) に切り替えることができます。ロールを引き受けるには、 または AWS API オペレーションを AWS CLI 呼び出すか、カスタム URL を使用します。ロールを使用する方法の詳細については、「IAM ユーザーガイド」の「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 ロールと一時的な認証情報は、次の状況で役立ちます:

- フェデレーションユーザーアクセス – フェデレーティッド ID に許可を割り当てるには、ロールを作成してそのロールの許可を定義します。フェデレーティッド ID が認証されると、その ID はロールに関連付けられ、ロールで定義されている許可が付与されます。フェデレーションのロールについては、「IAM ユーザーガイド」の「サードパーティー ID プロバイダー (フェデレーション) 用のロールを作成する」を参照してください。IAM Identity Center を使用する場合は、許可セットを設定します。アイデンティティが認証後にアクセスできるものを制御するため、IAM Identity Center は、権限セットを IAM のロールに関連付けます。アクセス許可セットの詳細については、「AWS IAM Identity Center User Guide」の「Permission sets」を参照してください。
- 一時的な IAM ユーザー権限 - IAM ユーザーまたはロールは、特定のタスクに対して複数の異なる権限を一時的に IAM ロールで引き受けることができます。
- クロスアカウントアクセス - IAM ロールを使用して、自分のアカウントのリソースにアクセスすることを、別のアカウントの人物 (信頼済みプリンシパル) に許可できます。クロスアカウントアクセス権を付与する主な方法は、ロールを使用することです。ただし、一部の では AWS のサービス、 (ロールをプロキシとして使用する代わりに) リソースに直接ポリシーをアタッチできます。クロスアカウントアクセスにおけるロールとリソースベースのポリシーの違いについては、「IAM ユーザーガイド」の「IAM でのクロスアカウントのリソースへのアクセス」を参照してください。
- クロスサービスアクセス — 一部の では、他の の機能 AWS のサービス を使用します AWS のサービス。例えば、あるサービスで呼び出しを行うと、通常そのサービスによって Amazon EC2

でアプリケーションが実行されたり、Amazon S3 にオブジェクトが保存されたりします。サービスでは、呼び出し元プリンシパルの許可、サービスロール、またはサービスリンクロールを使用してこれを行う場合があります。

- 転送アクセスセッション (FAS) – IAM ユーザーまたはロールを使用してアクションを実行すると AWS、プリンシパルと見なされます。一部のサービスを使用する際に、アクションを実行することで、別のサービスの別のアクションがトリガーされることがあります。FAS は、 を呼び出すプリンシパルのアクセス許可と AWS のサービス、ダウンストリームサービス AWS のサービス へのリクエストのリクエストをリクエストする を組み合わせて使用します。FAS リクエストは、サービスが他の AWS のサービス またはリソースとのやり取りを完了する必要があるリクエストを受け取った場合にのみ行われます。この場合、両方のアクションを実行するためのアクセス許可が必要です。FAS リクエストを行う際のポリシーの詳細については、「転送アクセスセッション」を参照してください。
- サービスロール - サービスがユーザーに代わってアクションを実行するために引き受ける IAM ロールです。IAM 管理者は、IAM 内からサービスロールを作成、変更、削除することができます。詳細については、「IAM ユーザーガイド」の「AWS のサービスに許可を委任するロールを作成する」を参照してください。
- サービスにリンクされたロール – サービスにリンクされたロールは、 にリンクされたサービスロールの一種です AWS のサービス。サービスは、ユーザーに代わってアクションを実行するロールを引き受けることができます。サービスにリンクされたロールは に表示され AWS アカウント 、 サービスによって所有されます。IAM 管理者は、サービスリンクロールのアクセス許可を表示できますが、編集することはできません。

- Amazon EC2 で実行されているアプリケーション – IAM ロールを使用して、EC2 インスタンスで実行され、 AWS CLI または AWS API リクエストを実行しているアプリケーションの一時的な認証情報を管理できます。これは、EC2 インスタンス内でのアクセスキーの保存に推奨されます。EC2 インスタンスに AWS ロールを割り当て、そのすべてのアプリケーションで使用できるようにするには、インスタンスにアタッチされたインスタンスプロファイルを作成します。インスタンスプロファイルにはロールが含まれ、EC2 インスタンスで実行されるプログラムは一時的な認証情報を取得できます。詳細については、「IAM ユーザーガイド」の「Amazon EC2 インスタンスで実行されるアプリケーションに IAM ロールを使用して許可を付与する」を参照してください。

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には AWS 、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 のオブジェクト AWS であり、アイデンティティまたはリソースに関連付けられると、

そのアクセス許可を定義します。 は、プリンシパル (ユーザー、ルートユーザー、またはロールセッション) がリクエストを行うときに、これらのポリシー AWS を評価します。ポリシーでの権限により、リクエストが許可されるか拒否されるかが決まります。ほとんどのポリシーは JSON ドキュメント AWS として に保存されます。JSON ポリシードキュメントの構造と内容の詳細については、IAM ユーザーガイドの JSON ポリシー概要を参照してください。

管理者は JSON AWS ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどのリソースに対してどのような条件下でアクションを実行できるかということです。

デフォルトでは、ユーザーやロールに権限はありません。IAM 管理者は、リソースで必要なアクションを実行するための権限をユーザーに付与する IAM ポリシーを作成できます。その後、管理者はロールに IAM ポリシーを追加し、ユーザーはロールを引き受けることができます。

IAM ポリシーは、オペレーションの実行方法を問わず、アクションの許可を定義します。例えば、`iam:GetRole` アクションを許可するポリシーがあるとします。そのポリシーを持つユーザーは、 AWS Management Console、、 AWS CLIまたは AWS API からロール情報を取得できます。

アイデンティティベースのポリシー

アイデンティティベースポリシーは、IAM ユーザーグループ、ユーザーのグループ、ロールなど、アイデンティティにアタッチできる JSON 許可ポリシードキュメントです。これらのポリシーは、ユーザーとロールが実行できるアクション、リソース、および条件をコントロールします。アイデンティティベース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、さらにインラインポリシーまたはマネージドポリシーに分類できます。インラインポリシーは、単一のユーザー、グループ、またはロールに直接埋め込まれています。管理ポリシーは、 内の複数のユーザー、グループ、ロールにアタッチできるスタンドアロンポリシーです AWS アカウント。管理ポリシーには、 AWS 管理ポリシーとカスタマー管理ポリシーが含まれます。マネージドポリシーまたはインラインポリシーのいずれかを選択する方法については、「IAM ユーザーガイド」の「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。

リソースベースのポリシー

リソースベースのポリシーは、リソースに添付する JSON ポリシードキュメントです。リソースベースのポリシーには例として、IAM ロールの信頼ポリシーや Amazon S3 バケットポリシーがあげられます。リソースベースのポリシーをサポートするサービスでは、サービス管理者はポリシーを

使用して特定のリソースへのアクセスを制御できます。ポリシーがアタッチされているリソースの場合、指定されたプリンシパルがそのリソースに対して実行できるアクションと条件は、ポリシーによって定義されます。リソースベースのポリシーでは、プリンシパルを指定する必要があります。プリンシパルには、アカウント、ユーザー、ロール、フェデレーティッドユーザー、または を含めることができます AWS のサービス。

リソースベースのポリシーは、そのサービス内にあるインラインポリシーです。リソースベースのポリシーでは、IAM の AWS マネージドポリシーを使用できません。

アクセスコントロールリスト (ACL)

アクセスコントロールリスト (ACL) は、どのプリンシパル (アカウントメンバー、ユーザー、またはロール) がリソースにアクセスするための許可を持つかを制御します。ACL はリソースベースのポリシーに似ていますが、JSON ポリシードキュメント形式は使用しません。

Amazon S3、 AWS WAF、および Amazon VPC は、ACLs。ACL の詳細については、「Amazon Simple Storage Service デベロッパーガイド」の「アクセスコントロールリスト (ACL) の概要」を参照してください。

その他のポリシータイプ

AWS は、一般的ではない追加のポリシータイプをサポートしています。これらのポリシータイプでは、より一般的なポリシータイプで付与された最大の権限を設定できます。

- アクセス許可の境界 - アクセス許可の境界は、アイデンティティベースポリシーによって IAM エンティティ (IAM ユーザーまたはロール) に付与できる権限の上限を設定する高度な機能です。エンティティにアクセス許可の境界を設定できます。結果として得られる権限は、エンティティのアイデンティティベースポリシーとそのアクセス許可の境界の共通部分になります。`Principal` フィールドでユーザーまたはロールを指定するリソースベースのポリシーでは、アクセス許可の境界は制限されません。これらのポリシーのいずれかを明示的に拒否した場合、権限は無効になります。アクセス許可の境界の詳細については、「IAM ユーザーガイド」の「IAM エンティティのアクセス許可の境界」を参照してください。
- サービスコントロールポリシー (SCPs) – SCPsは、 の組織または組織単位 (OU) の最大アクセス許可を指定する JSON ポリシーです AWS Organizations。 AWS Organizations は、ビジネスが所有する複数の AWS アカウント をグループ化して一元管理するためのサービスです。組織内のすべての機能を有効にすると、サービスコントロールポリシー (SCP) を一部またはすべてのアカウントに適用できます。SCP は、各 を含むメンバーアカウントのエンティティのアクセス許可を制限します AWS アカウントのルートユーザー。Organizations と SCP の詳細については、「AWS

Organizations ユーザーガイド」の「サービスコントロールポリシー (SCP)」を参照してください。

- リソースコントロールポリシー (RCP) – RCP は、所有する各リソースにアタッチされた IAM ポリシーを更新することなく、アカウント内のリソースに利用可能な最大数のアクセス許可を設定するために使用できる JSON ポリシーです。RCP は、メンバーアカウントのリソースのアクセス許可を制限し、組織に属しているかどうかにかかわらず AWS アカウントのルートユーザー、 を含む ID の有効なアクセス許可に影響を与える可能性があります。RCP をサポートする のリストなど、Organizations と RCP の詳細については、AWS Organizations 「 ユーザーガイド AWS のサービス 」の「リソースコントロールポリシー (RCPs」を参照してください。 RCPs
- セッションポリシー - セッションポリシーは、ロールまたはフェデレーションユーザーの一時的なセッションをプログラムで作成する際にパラメータとして渡す高度なポリシーです。結果としてセッションの権限は、ユーザーまたはロールのアイデンティティベースポリシーとセッションポリシーの共通部分になります。また、リソースベースのポリシーから権限が派生する場合もあります。これらのポリシーのいずれかを明示的に拒否した場合、権限は無効になります。詳細については、「IAM ユーザーガイド」の「セッションポリシー」を参照してください。

複数のポリシータイプ

1 つのリクエストに複数のタイプのポリシーが適用されると、結果として作成される権限を理解するのがさらに難しくなります。複数のポリシータイプが関係する場合に がリクエストを許可するかどうか AWS を決定する方法については、「IAM ユーザーガイド」の「ポリシー評価ロジック」を参照してください。

App Runner と IAM の連携方法

IAM を使用して へのアクセスを管理する前に AWS App Runner、App Runner で使用できる IAM 機能を理解しておく必要があります。App Runner およびその他の AWS のサービスが IAM と連携する方法の概要を把握するには、「IAM ユーザーガイド」のAWS 「IAM と連携する のサービス」を参照してください。

その他の App Runner セキュリティトピックについては、「」を参照してくださいセキュリティ。

トピック

- App Runner アイデンティティベースのポリシー
- App Runner リソースベースのポリシー
- App Runner タグに基づく認可

- App Runner ユーザーのアクセス許可
- App Runner IAM ロール

App Runner 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。App Runner は、特定のアクション、リソース、および条件キーをサポートしています。JSON ポリシーで使用するすべての要素については、「IAM ユーザーガイド」の「IAM JSON ポリシー要素のリファレンス」を参照してください。

アクション

管理者は JSON AWS ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどのリソースに対してどのような条件下でアクションを実行できるかということです。

JSON ポリシーの `Action` 要素にはポリシー内のアクセスを許可または拒否するために使用できるアクションが記述されます。ポリシーアクションの名前は通常、関連する AWS API オペレーションと同じです。一致する API オペレーションのない許可のみのアクションなど、いくつかの例外があります。また、ポリシーに複数のアクションが必要なオペレーションもあります。これらの追加アクションは依存アクションと呼ばれます。

このアクションは関連付けられたオペレーションを実行するためのアクセス許可を付与するポリシーで使用されます。

App Runner 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 を使用します`apprunner:`。たとえば、 Amazon EC2 `RunInstances` API オペレーションで Amazon EC2 インスタンスを実行するためのアクセス許可をユーザーに付与するには、ポリシーに `ec2:RunInstances` 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` エレメントを含める必要があります。App Runner は、このサービスで実行できるタスクを記述する独自のアクションのセットを定義します。

単一のステートメントに複数のアクションを指定するには次のようにコンマで区切ります。

```
"Action": [
   "apprunner:CreateService",
   "apprunner:CreateConnection"
]
```

ワイルドカード (*) を使用して複数アクションを指定できます。例えば、Describe 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": "apprunner:Describe*"
```

App Runner アクションのリストを確認するには、「サービス認可リファレンス」の「 で定義されるアクション AWS App Runner」を参照してください。

リソース

管理者は JSON AWS ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルが、どのリソースに対してどのような条件下でアクションを実行できるかということです。

Resource JSON ポリシー要素はアクションが適用されるオブジェクトを指定します。ステートメントにはResource または NotResource 要素を含める必要があります。ベストプラクティスとして、Amazon リソースネーム (ARN) を使用してリソースを指定します。これは、リソースレベルの許可と呼ばれる特定のリソースタイプをサポートするアクションに対して実行できます。

オペレーションのリスト化など、リソースレベルの権限をサポートしないアクションの場合は、ステートメントがすべてのリソースに適用されることを示すために、ワイルドカード (*) を使用します。

```
"Resource": "*"
```

App Runner リソースの ARN 構造は次のとおりです。

```
arn:aws:apprunner:region:account-id:resource-type/resource-name[/resource-id]
```

ARN の形式の詳細については、の「Amazon リソースネーム (ARNs) と AWS サービスの名前空間」を参照してくださいAWS 全般のリファレンス。

たとえば、 ステートメントで my-serviceサービスを指定するには、次の ARN を使用します。

```
"Resource": "arn:aws:apprunner:us-east-1:123456789012:service/my-service"
```

特定のアカウントに属するすべてのサービスを指定するには、ワイルドカード (*) を使用します。

```
"Resource": "arn:aws:apprunner:us-east-1:123456789012:service/*"
```

リソースを作成するためのアクションなど、一部の App Runner アクションは、特定のリソースで実行できません。このような場合はワイルドカード *を使用する必要があります。

```
"Resource": "*"
```

App Runner リソースタイプとその ARNs「 で定義されるリソース AWS App Runner」を参照してください。 どのアクションで各リソースの ARN を指定できるかについては、「AWS App Runnerで定義されるアクション」を参照してください。

条件キー

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。

`Condition` 要素 (または `Condition` ブロック) を使用すると、ステートメントが有効な条件を指定できます。`Condition` 要素はオプションです。イコールや未満などの 条件演算子 を使用して条件式を作成して、ポリシーの条件とリクエスト内の値を一致させることができます。

1 つのステートメントに複数の `Condition` 要素を指定する場合、または 1 つの `Condition` 要素に複数のキーを指定する場合、 AWS では `AND` 論理演算子を使用してそれらを評価します。1 つの条件キーに複数の値を指定すると、 は論理`OR`オペレーションを使用して条件 AWS を評価します。ステートメントの権限が付与される前にすべての条件が満たされる必要があります。

条件を指定する際にプレースホルダー変数も使用できます。例えば IAM ユーザーに、IAM ユーザー名がタグ付けされている場合のみリソースにアクセスできる権限を付与することができます。詳細については、「IAM ユーザーガイド」の「IAM ポリシーの要素: 変数およびタグ」を参照してください。

AWS は、グローバル条件キーとサービス固有の条件キーをサポートしています。すべての AWS グローバル条件キーを確認するには、「IAM ユーザーガイド」のAWS 「 グローバル条件コンテキストキー」を参照してください。

App Runner は、いくつかのグローバル条件キーの使用をサポートしています。すべての AWS グローバル条件キーを確認するには、「IAM ユーザーガイド」のAWS 「グローバル条件コンテキストキー」を参照してください。

App Runner は、サービス固有の条件キーのセットを定義します。さらに、App Runner は、条件キーを使用して実装されるタグベースのアクセスコントロールをサポートしています。詳細については、「the section called “App Runner タグに基づく認可”」を参照してください。

App Runner の条件キーのリストを確認するには、「サービス認可リファレンス」の「 の条件キー AWS App Runner」を参照してください。条件キーを使用できるアクションとリソースについては、「 で定義されるアクション AWS App Runner」を参照してください。

例

App Runner 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App Runner アイデンティティベースのポリシーの例。

App Runner リソースベースのポリシー

App Runner はリソースベースのポリシーをサポートしていません。

App Runner タグに基づく認可

App Runner リソースにタグをアタッチするか、App Runner へのリクエストでタグを渡すことができます。タグに基づいてアクセスを制御するには`apprunner: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。App Runner 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the section called “設定”。

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ポリシーの例を表示するには、「タグに基づく App Runner サービスへのアクセスの制御」を参照してください。

App Runner ユーザーのアクセス許可

App Runner を使用するには、IAM ユーザーに App Runner アクションへのアクセス許可が必要です。ユーザーに許可を付与する一般的な方法は、IAM ユーザーまたはグループにポリシーをアタッチすることです。ユーザーアクセス許可の管理の詳細については、「IAM ユーザーガイド」の「IAM ユーザーのアクセス許可の変更」を参照してください。

App Runner には、ユーザーにアタッチできる 2 つの管理ポリシーが用意されています。

- `AWSAppRunnerReadOnlyAccess` – App Runner リソースの詳細を一覧表示および表示するアクセス許可を付与します。
- `AWSAppRunnerFullAccess` – すべての App Runner アクションにアクセス許可を付与します。

ユーザーのアクセス許可をより詳細に制御するには、カスタムポリシーを作成してユーザーにアタッチします。詳細については、「IAM ユーザーガイド」の「IAM ポリシーの作成」を参照してください。

ユーザーポリシーの例については、「」を参照してくださいthe section called “ユーザーポリシー”。

AWSAppRunnerReadOnlyAccess

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "apprunner:List*",
        "apprunner:Describe*"
      ],
      "Resource": "*"
    }
  ]
}
```

AWSAppRunnerFullAccess

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "iam:CreateServiceLinkedRole",
      "Resource": [
        "arn:aws:iam::*:role/aws-service-role/apprunner.amazonaws.com/
AWSServiceRoleForAppRunner",
        "arn:aws:iam::*:role/aws-service-role/networking.apprunner.amazonaws.com/
AWSServiceRoleForAppRunnerNetworking"
      ],
      "Condition": {
        "StringLike": {
          "iam:AWSServiceName": [
            "apprunner.amazonaws.com",
            "networking.apprunner.amazonaws.com"
          ]
        }
```

```
      }
    },
    {
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "iam:PassedToService": "apprunner.amazonaws.com"
        }
      }
    },
    {
      "Sid": "AppRunnerAdminAccess",
      "Effect": "Allow",
      "Action": "apprunner:*",
      "Resource": "*"
    }
  ]
}
```

App Runner IAM ロール

IAM ロールは、特定のアクセス許可 AWS アカウント を持つ 内のエンティティです。

サービスにリンクされた役割

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。

App Runner 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。App Runner のサービスにリンクされたロールの作成または管理については、「」を参照してくださいthe section called “サービスにリンクされたロールの使用”。

サービス役割

この機能により、ユーザーに代わってサービスがサービス役割を引き受けることが許可されます。この役割により、サービスがお客様に代わって他のサービスのリソースにアクセスし、アクションを完了することが許可されます。サービス役割はIAM アカウントに表示され、アカウントによって所有

されます。つまり、IAM ユーザーはこのロールのアクセス許可を変更できます。ただし、それにより、サービスの機能が損なわれる場合があります。

App Runner は、いくつかのサービスロールをサポートしています。

アクセスロール

アクセスロールは、App Runner がアカウントの Amazon Elastic Container Registry (Amazon ECR) 内のイメージにアクセスするために使用するロールです。Amazon ECR 内のイメージにアクセスするために必要であり、Amazon ECR Public では必要ありません。Amazon ECR のイメージに基づいてサービスを作成する前に、IAM を使用してサービスロールを作成し、その中に `AWSAppRunnerServicePolicyForECRAccess` マネージドポリシーを使用します。その後、SourceConfiguration パラメータの AuthenticationConfiguration メンバーで CreateService API を呼び出すとき、または App Runner コンソールを使用してサービスを作成するときに、このロールを App Runner に渡すことができます。

AWSAppRunnerServicePolicyForECRAccess

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ecr:GetDownloadUrlForLayer",
        "ecr:BatchCheckLayerAvailability",
        "ecr:BatchGetImage",
        "ecr:DescribeImages",
        "ecr:GetAuthorizationToken"
      ],
      "Resource": "*"
    }
  ]
}
```

> **Note**
>
> アクセスロールに独自のカスタムポリシーを作成する場合は、必ず `ecr:GetAuthorizationToken`アクション`"Resource": "*"`に を指定してください。

トークンは、アクセスできる任意の Amazon ECR レジストリへのアクセスに使用できます。

アクセスロールを作成するときは、App Runner サービスプリンシパルを信頼されたエンティティ`build.apprunner.amazonaws.com`として宣言する信頼ポリシーを必ず追加してください。

アクセスロールの信頼ポリシー

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "build.apprunner.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

App Runner コンソールを使用してサービスを作成する場合、コンソールは自動的にアクセスロールを作成し、新しいサービス用に選択できます。コンソールにはアカウント内の他のロールも一覧表示され、必要に応じて別のロールを選択できます。

インスタンスロール

インスタンスロールは、App Runner がサービスのコンピューティングインスタンスに必要な AWS サービスアクションへのアクセス許可を提供するために使用するオプションのロールです。アプリケーションコードが AWS アクション (APIs) を呼び出す場合は、App Runner にインスタンスロールを提供する必要があります。必要なアクセス許可をインスタンスロールに埋め込むか、独自のカスタムポリシーを作成してインスタンスロールで使用します。コードが使用する呼び出しを予測する方法はありません。したがって、この目的のために管理ポリシーは提供しません。

App Runner サービスを作成する前に、IAM を使用して、必要なカスタムポリシーまたは埋め込みポリシーを持つサービスロールを作成します。その後、InstanceConfiguration パラメータ`InstanceRoleArn`のメンバーで CreateService API を呼び出すとき、または App Runner コンソールを使用してサービスを作成するときに、このロールをインスタンスロールとして App Runner に渡すことができます。

インスタンスロールを作成するときは、App Runner サービスプリンシパルを信頼されたエンティティ`tasks.apprunner.amazonaws.com`として宣言する信頼ポリシーを必ず追加してください。

インスタンスロールの信頼ポリシー

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "tasks.apprunner.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

App Runner コンソールを使用してサービスを作成する場合、コンソールにはアカウントのロールが一覧表示され、この目的のために作成したロールを選択できます。

サービスの作成については、「」を参照してくださいthe section called “作成”。

App Runner アイデンティティベースのポリシーの例

デフォルトでは、IAM ユーザーとロールには AWS App Runner リソースを作成または変更するアクセス許可はありません。また、、 AWS Management Console 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、ユーザーとロールに必要な、指定されたリソースで特定の API オペレーションを実行する権限をユーザーとロールに付与する IAM ポリシーを作成する必要があります。続いて、管理者はそれらの権限が必要な IAM ユーザーまたはグループにそのポリシーをアタッチする必要があります。

JSON ポリシードキュメントのこれらの例を使用して、IAM アイデンティティベースのポリシーを作成する方法については、「IAM ユーザーガイド」の「JSON タブでのポリシーの作成」を参照してください。

その他の App Runner セキュリティトピックについては、「」を参照してくださいセキュリティ。

トピック

- ポリシーに関するベストプラクティス

- ユーザーポリシー
- タグに基づく App Runner サービスへのアクセスの制御

ポリシーに関するベストプラクティス

ID ベースのポリシーは、ユーザーのアカウントで誰かが App Runner リソースを作成、アクセス、または削除できるどうかを決定します。これらのアクションを実行すると、 AWS アカウントに料金が発生する可能性があります。アイデンティティベースポリシーを作成したり編集したりする際には、以下のガイドラインと推奨事項に従ってください:

- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する – ユーザーとワークロードにアクセス許可を付与するには、多くの一般的なユースケースにアクセス許可を付与するAWS 管理ポリシーを使用します。これらは で使用できます AWS アカウント。ユースケースに固有の AWS カスタマー管理ポリシーを定義して、アクセス許可をさらに減らすことをお勧めします。詳細については、「IAM ユーザーガイド」の「AWS マネージドポリシー」または「ジョブ機能の AWS マネージドポリシー」を参照してください。
- 最小特権を適用する – IAM ポリシーで許可を設定する場合は、タスクの実行に必要な許可のみを付与します。これを行うには、特定の条件下で特定のリソースに対して実行できるアクションを定義します。これは、最小特権アクセス許可とも呼ばれています。IAM を使用して許可を適用する方法の詳細については、「IAM ユーザーガイド」の「IAM でのポリシーとアクセス許可」を参照してください。
- IAM ポリシーで条件を使用してアクセスをさらに制限する - ポリシーに条件を追加して、アクションやリソースへのアクセスを制限できます。例えば、ポリシー条件を記述して、すべてのリクエストを SSL を使用して送信するように指定できます。条件を使用して、サービスアクションが などの特定の を通じて使用される場合に AWS のサービス、サービスアクションへのアクセスを許可することもできます AWS CloudFormation。詳細については、「IAM ユーザーガイド」の「IAM JSON ポリシー要素:条件」を参照してください。
- IAM Access Analyzer を使用して IAM ポリシーを検証し、安全で機能的な権限を確保する - IAM Access Analyzer は、新規および既存のポリシーを検証して、ポリシーが IAM ポリシー言語 (JSON) および IAM のベストプラクティスに準拠するようにします。IAM アクセスアナライザーは 100 を超えるポリシーチェックと実用的な推奨事項を提供し、安全で機能的なポリシーの作成をサポートします。詳細については、「IAM ユーザーガイド」の「IAM Access Analyzer でポリシーを検証する」を参照してください。
- 多要素認証 (MFA) を要求する – で IAM ユーザーまたはルートユーザーを必要とするシナリオがある場合は AWS アカウント、セキュリティを強化するために MFA を有効にします。API オペレーションが呼び出されるときに MFA を必須にするには、ポリシーに MFA 条件を追加します。詳細

については、「IAM ユーザーガイド」の「MFA を使用した安全な API アクセス」を参照してください。

IAM でのベストプラクティスの詳細については、IAM ユーザーガイドの IAM でのセキュリティのベストプラクティスを参照してください。

ユーザーポリシー

App Runner コンソールにアクセスするには、IAM ユーザーに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、 の App Runner リソースの詳細を一覧表示および表示できます AWS アカウント。最小限必要なアクセス許可よりも制限されたアイデンティティベースのポリシーを作成すると、そのポリシーを持つユーザーに対してコンソールは意図したとおりに機能しません。

App Runner には、ユーザーにアタッチできる 2 つの管理ポリシーが用意されています。

- `AWSAppRunnerReadOnlyAccess` – App Runner リソースの詳細を一覧表示および表示するアクセス許可を付与します。
- `AWSAppRunnerFullAccess` – すべての App Runner アクションにアクセス許可を付与します。

ユーザーが App Runner コンソールを使用できるようにするには、少なくとも、`AWSAppRunnerReadOnlyAccess`管理ポリシーをユーザーにアタッチします。代わりに`AWSAppRunnerFullAccess`管理ポリシーをアタッチするか、特定のアクセス許可を追加して、ユーザーがリソースを作成、変更、削除できるようにします。詳細については、「IAM ユーザーガイド」の「ユーザーへのアクセス許可の追加」を参照してください。

AWS CLI または AWS API のみを呼び出すユーザーには、最小限のコンソールアクセス許可を付与する必要はありません。代わりに、ユーザーに実行を許可する 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を許可します。

次の例は、カスタムユーザーポリシーを示しています。独自のカスタムユーザーポリシーを定義するための出発点として使用できます。例をコピーするか、アクションを削除するか、リソースの範囲を絞り込み、条件を追加します。

例: コンソールと接続管理のユーザーポリシー

このポリシー例では、コンソールアクセスを有効にし、接続の作成と管理を許可します。App Runner サービスの作成と管理は許可されません。これは、ソースコードアセットへの App Runner サービスアクセスを管理するロールを持つユーザーにアタッチできます。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "apprunner:List*",
        "apprunner:Describe*",
        "apprunner:CreateConnection",
        "apprunner:DeleteConnection"
      ],
      "Resource": "*"
    }
  ]
}
```

例: 条件キーを使用するユーザーポリシー

このセクションの例では、一部のリソースプロパティまたはアクションパラメータに依存する条件付きアクセス許可を示します。

このポリシー例では、App Runner サービスの作成を有効にしますが、 という名前の接続の使用を拒否しますprod。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowCreateAppRunnerServiceWithNonProdConnections",
      "Effect": "Allow",
      "Action": "apprunner:CreateService",
      "Resource": "*",
      "Condition": {
        "ArnNotLike": {
          "apprunner:ConnectionArn": "arn:aws:apprunner:*:*:connection/prod/*"
        }
      }
    }
  ]
}
```

このポリシー例では、 という名前の自動スケーリング設定preprodでのみ、 という名前の App Runner サービスの更新を有効にしますpreprod。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowUpdatePreProdAppRunnerServiceWithPreProdASConfig",
      "Effect": "Allow",
      "Action": "apprunner:UpdateService",
      "Resource": "arn:aws:apprunner:*:*:service/preprod/*",
      "Condition": {
        "ArnLike": {
          "apprunner:AutoScalingConfigurationArn":
 "arn:aws:apprunner:*:*:autoscalingconfiguration/preprod/*"
        }
      }
    }
  ]
}
```

タグに基づく App Runner サービスへのアクセスの制御

アイデンティティベースのポリシーの条件を使用して、タグに基づいて App Runner リソースへのアクセスを制御できます。この例では、App Runner サービスの削除を許可するポリシーを作成する方法を示します。ただし、アクセス許可は、サービスタグ Owner にそのユーザーのユーザー名の値がある場合のみ、付与されます。このポリシーでは、このアクションをコンソールで実行するために必要なアクセス許可も付与します。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ListServicesInConsole",
      "Effect": "Allow",
      "Action": "apprunner:ListServices",
      "Resource": "*"
    },
    {
      "Sid": "DeleteServiceIfOwner",
      "Effect": "Allow",
      "Action": "apprunner:DeleteService",
```

```
      "Resource": "arn:aws:apprunner:*:*:service/*",
      "Condition": {
        "StringEquals": {"apprunner:ResourceTag/Owner": "${aws:username}"}
      }
    }
  ]
}
```

このポリシーをアカウントの IAM ユーザーにアタッチできます。という名前のユーザーが App Runner サービスを削除`richard-roe`しようとする場合は、サービスに `Owner=richard-roe`または のタグを付ける必要があります`owner=richard-roe`。それ以外の場合、アクセスは拒否されます。条件キー名では大文字と小文字が区別されないため、条件タグキー `Owner` は `Owner` と `owner` の両方に一致します。詳細については、「IAM ユーザーガイド」の「IAM JSON ポリシー要素: 条件」を参照してください。

App Runner のサービスにリンクされたロールの使用

AWS App Runner 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、App Runner に直接リンクされた一意のタイプの IAM ロールです。サービスにリンクされたロールは App Runner によって事前定義されており、ユーザーに代わってサービスから他の AWS の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。

トピック

- ロールを管理に使用する
- ネットワークに ロールを使用する

ロールを管理に使用する

AWS App Runner 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、App Runner に直接リンクされた一意のタイプの IAM ロールです。サービスにリンクされたロールは App Runner によって事前定義されており、ユーザーに代わってサービスから他の AWS の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。

サービスにリンクされたロールを使用すると、必要なアクセス許可を手動で追加する必要がなくなるため、App Runner の設定が簡単になります。App Runner 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ます。特に定義されている場合を除き、App Runner 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。

サービスリンクロールを削除するには、最初に関連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を誤って削除することがなくなるため、App Runner 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する他のサービスについては、「IAM と連携するAWS サービス」を参照して、サービスにリンクされたロール列がはいになっているサービスを見つけてください。サービスにリンクされたロールに関するドキュメントをサービスで表示するには、はいリンクを選択します。

App Runner のサービスにリンクされたロールのアクセス許可

App Runner は、AWSServiceRoleForAppRunner という名前のサービスにリンクされたロールを使用します。

このロールにより、App Runner は次のタスクを実行できます。

- Amazon CloudWatch Logs Logs ロググループにログをプッシュします。
- Amazon Elastic Container Registry (Amazon ECR) イメージプッシュをサブスクライブする Amazon CloudWatch Events ルールを作成します。
- トレース情報を に送信します AWS X-Ray。

AWSServiceRoleForAppRunner サービスにリンクされたロールは、次のサービスを信頼してロールを引き受けます。

- `apprunner.amazonaws.com`

AWSServiceRoleForAppRunner サービスにリンクされたロールのアクセス許可ポリシーには、App Runner がユーザーに代わってアクションを実行するために必要なすべてのアクセス許可が含まれています。

AppRunnerServiceRolePolicy マネージドポリシー

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

```
      "Action": [
        "logs:CreateLogGroup",
        "logs:PutRetentionPolicy"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:logs:*:*:log-group:/aws/apprunner/*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogStreams"
      ],
      "Resource": [
        "arn:aws:logs:*:*:log-group:/aws/apprunner/*:log-stream:*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "events:PutRule",
        "events:PutTargets",
        "events:DeleteRule",
        "events:RemoveTargets",
        "events:DescribeRule",
        "events:EnableRule",
        "events:DisableRule"
      ],
      "Resource": "arn:aws:events:*:*:rule/AWSAppRunnerManagedRule*"
    }
  ]
}
```

X-Ray トレースのポリシー

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "xray:PutTraceSegments",
```

```
        "xray:PutTelemetryRecords",
        "xray:GetSamplingRules",
        "xray:GetSamplingTargets",
        "xray:GetSamplingStatisticSummaries"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

サービスリンク役割の作成、編集、削除を IAM エンティティ (ユーザー、グループ、役割など) 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。

App Runner 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。 AWS Management Console、、 AWS CLIまたは AWS API で App Runner サービスを作成すると、App Runner によって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。App Runner サービスを作成すると、App Runner によってサービスにリンクされたロールが再度作成されます。

App Runner のサービスにリンクされたロールの編集

App Runner では、AWSServiceRoleForAppRunner サービスにリンクされたロールを編集することはできません。サービスリンクロールの作成後は、さまざまなエンティティがロールを参照する可能性があるため、ロール名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「サービスにリンクされたロールの編集」を参照してください。

App Runner のサービスにリンクされたロールの削除

サービスリンクロールを必要とする機能やサービスが不要になった場合は、ロールを削除することをお勧めします。そうすることで、モニタリングや保守が積極的に行われていない未使用のエンティティを排除できます。ただし、手動で削除する前に、サービスリンク役割をクリーンアップする必要があります。

サービスリンク役割のクリーンアップ

IAM を使用してサービスにリンクされた役割を削除するには最初に、その役割で使用されているリソースをすべて削除する必要があります。

App Runner では、これはアカウント内のすべての App Runner サービスを削除することを意味します。App Runner サービスの削除については、「」を参照してくださいthe section called “削除”。

> **Note**
> リソースを削除しようとしたときに App Runner 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。

サービスにリンクされたロールを手動で削除する

IAM コンソール、、または AWS API を使用して AWS CLI、AWSServiceRoleForAppRunner 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「サービスにリンクされたロールの削除」を参照してください。

App Runner 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

App Runner は、サービスが利用可能なすべてのリージョンで、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 全般のリファレンス」の「AWS App Runner エンドポイントとクォータ」を参照してください。

ネットワークに ロールを使用する

AWS App Runner 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、App Runner に直接リンクされた一意のタイプの IAM ロールです。サービスにリンクされたロールは App Runner によって事前定義されており、ユーザーに代わってサービスから他の AWS の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。

サービスにリンクされたロールを使用すると、必要なアクセス許可を手動で追加する必要がなくなるため、App Runner の設定が簡単になります。App Runner 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ます。特に定義されている場合を除き、App Runner 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。

サービスリンクロールを削除するには、最初に関連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を誤って削除することがなくなるため、App Runner 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する他のサービスについては、「IAM と連携するAWS サービス」を参照して、サービスにリンクされたロール列がはいになっているサービスを見つけてください。サービスにリンクされたロールに関するドキュメントをサービスで表示するには、はいリンクを選択します。

App Runner のサービスにリンクされたロールのアクセス許可

App Runner は、AWSServiceRoleForAppRunnerNetworking という名前のサービスにリンクされたロールを使用します。

このロールにより、App Runner は次のタスクを実行できます。

- VPC を App Runner サービスにアタッチし、ネットワークインターフェイスを管理します。

AWSServiceRoleForAppRunnerNetworking サービスにリンクされたロールは、次のサービスを信頼してロールを引き受けます。

- `networking.apprunner.amazonaws.com`

AppRunnerNetworkingServiceRolePolicy という名前のロールアクセス許可ポリシーには、App Runner がユーザーに代わってアクションを実行するために必要なすべてのアクセス許可が含まれています。

AppRunnerNetworkingServiceRolePolicy

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVpcs",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups"
      ],
```

```
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "ec2:CreateNetworkInterface",
      "Resource": "*",
      "Condition": {
        "ForAllValues:StringEquals": {
          "aws:TagKeys": [
            "AWSAppRunnerManaged"
          ]
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": "ec2:CreateTags",
      "Resource": "arn:aws:ec2:*:*:network-interface/*",
      "Condition": {
        "StringEquals": {
          "ec2:CreateAction": "CreateNetworkInterface"
        },
        "StringLike": {
          "aws:RequestTag/AWSAppRunnerManaged": "*"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": "ec2:DeleteNetworkInterface",
      "Resource": "*",
      "Condition": {
        "Null": {
          "ec2:ResourceTag/AWSAppRunnerManaged": "false"
        }
      }
    }
  ]
}
```

サービスリンク役割の作成、編集、削除を IAM エンティティ (ユーザー、グループ、役割など) 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。

App Runner 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。 AWS Management Console、、 AWS CLIまたは AWS API で VPC コネクタを作成すると、App Runner によって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。VPC コネクタを作成すると、App Runner によってサービスにリンクされたロールが再度作成されます。

App Runner のサービスにリンクされたロールの編集

App Runner では、AWSServiceRoleForAppRunnerNetworking サービスにリンクされたロールを編集することはできません。サービスリンクロールの作成後は、さまざまなエンティティがロールを参照する可能性があるため、ロール名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「サービスにリンクされたロールの編集」を参照してください。

App Runner のサービスにリンクされたロールの削除

サービスリンクロールを必要とする機能やサービスが不要になった場合は、ロールを削除することをお勧めします。そうすることで、モニタリングや保守が積極的に行われていない未使用のエンティティを排除できます。ただし、手動で削除する前に、サービスリンク役割をクリーンアップする必要があります。

サービスにリンクされたロールのクリーンアップ

IAM を使用してサービスにリンクされた役割を削除するには最初に、その役割で使用されているリソースをすべて削除する必要があります。

App Runner では、アカウント内のすべての App Runner サービスから VPC コネクタの関連付けを解除し、VPC コネクタを削除することを意味します。詳細については、「the section called “送信トラフィック”」を参照してください。

> **Note**
>
> リソースを削除しようとしたときに App Runner 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。

サービスリンクロールを手動で削除する

IAM コンソール、、または AWS API を使用して AWS CLI、AWSServiceRoleForAppRunnerNetworking サービスリンク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「サービスにリンクされたロールの削除」を参照してください。

App Runner 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

App Runner は、サービスが利用可能なすべてのリージョンで、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 全般のリファレンス」の「AWS App Runner エンドポイントとクォータ」を参照してください。

AWS の マネージドポリシー AWS App Runner

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、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るため、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 管理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 AWS のサービス が起動されたとき、または既存のサービスで新しい API オペレーションが利用可能になったときに、 AWS 管理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。

AWS マネージドポリシーに対する App Runner の更新

App Runner の AWS マネージドポリシーの更新に関する詳細を、このサービスがこれらの変更の追跡を開始した以降の分について表示します。このページの変更に関する自動通知については、App Runner 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
AWSAppRunnerReadOnlyAccess – 新しいポリシー	App Runner は、ユーザーが App Runner リソースの詳細を一覧表示および表示できるようにする新しいポリシーを追加しました。	2022 年 2 月 24 日
AWSAppRunnerFullAccess – 既存のポリシーの更新	App Runner は、 `iam:CreateServiceLinkedRole` アクションのリソースリストを更新して、`AWSServiceRoleForAppRunnerNetworking` サービスにリンクされたロールを作成できるようにしました。	2022 年 2 月 8 日
AppRunnerNetworkingServiceRolePolicy – 新しいポリシー	App Runner は、App Runner が Amazon Virtual Private Cloud を呼び出して VPC を App Runner サービスにアタッチし、App Runner サービスに代わってネットワークインターフェイスを管理できるようにする新しいポリシーを追加しました。ポリシーは、`AWSServiceRoleForAppRunnerNetworking` サービスにリンクされたロールで使用されます。	2022 年 2 月 8 日
AWSAppRunnerFullAccess – 新しいポリシー	App Runner は、ユーザーがすべての App Runner アクションを実行できるようにする新しいポリシーを追加しました。	2022 年 1 月 10 日
AppRunnerServiceRolePolicy – 新しいポリシー	App Runner は、App Runner が App Runner サービスに代わって Amazon CloudWatch Logs と Amazon CloudWatch Events を呼び出すことを許可する	2021 年 3 月 1 日

変更	説明	日付
	新しいポリシーを追加しました。ポリシーは、`AWSServiceRoleForAppRunner` サービスにリンクされたロールで使用されます。	
AWSAppRunnerServicePolicyForECRAccess – 新しいポリシー	App Runner は、App Runner がアカウントの Amazon Elastic Container Registry (Amazon ECR) イメージにアクセスできるようにする新しいポリシーを追加しました。	2021 年 3 月 1 日
App Runner が変更の追跡を開始しました	App Runner が AWS マネージドポリシーの変更の追跡を開始しました。	2021 年 3 月 1 日

App Runner 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、 と IAM の使用時に発生する可能性がある一般的な問題の診断 AWS App Runner と修正に役立ちます。

その他の App Runner セキュリティトピックについては、「」を参照してくださいセキュリティ。

トピック

- App Runner でアクションを実行する権限がない
- 自分の 以外のユーザーに App Runner リソース AWS アカウント へのアクセスを許可したい

App Runner でアクションを実行する権限がない

から、アクションを実行する権限がないと AWS Management Console 通知された場合は、管理者に連絡してサポートを依頼してください。管理者は、 AWS サインイン認証情報を提供したユーザーです。

次の例のエラーは、 という IAM `marymajor` ユーザーがコンソールを使用して App Runner サービスの詳細を表示しようとしているが、 アクセス`apprunner:DescribeService`許可がない場合に発生します。

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 apprunner:DescribeService on resource: my-example-service
```

この場合、Mary は、 `apprunner:DescribeService`アクションを使用して *`my-example-service`*リソースにアクセスできるようにポリシーを更新するように管理者に依頼します。

自分の 以外のユーザーに App Runner リソース AWS アカウント 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:

- App Runner 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[App Runner と IAM の連携方法](#)。
- 所有 AWS アカウント する 全体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 する別の の IAM ユーザーへのアクセスを提供する」を参照してください。
- リソースへのアクセスをサードパーティーに提供する方法については AWS アカウント、「IAM ユーザーガイド」の「サードパーティー AWS アカウント が所有する へのアクセスを提供する」を参照してください。
- ID フェデレーションを介してアクセスを提供する方法については、「IAM ユーザーガイド」の「外部で認証されたユーザー (ID フェデレーション) へのアクセスの許可」を参照してください。
- クロスアカウントアクセスにおけるロールとリソースベースのポリシーの使用方法の違いについては、「IAM ユーザーガイド」の「IAM でのクロスアカウントのリソースへのアクセス」を参照してください。

App Runner でのログ記録とモニタリング

モニタリングは、 AWS App Runner サービスの信頼性、可用性、パフォーマンスを維持する上で重要な部分です。 AWS ソリューションのすべての部分からモニタリングデータを収集することで、障害が発生した場合に、その障害をより簡単にデバッグできます。App Runner は、App Runner サービスをモニタリングし、潜在的なインシデントに対応するためのいくつかの AWS ツールと統合されています。

Amazon CloudWatch アラーム

Amazon CloudWatch アラームを使用すると、指定した期間にわたってサービスメトリクスを監視できます。メトリクスが特定の期間にわたって特定のしきい値を超えると、通知を受け取ります。

App Runner は、サービス全体と、ウェブサービスを実行するインスタンス (スケーリングユニット) に関するさまざまなメトリクスを収集します。詳細については、「メトリクス (CloudWatch)」を参照してください。

アプリケーションログ

App Runner は、アプリケーションコードの出力を収集し、Amazon CloudWatch Logs にストリーミングします。この出力の内容はユーザー次第です。例えば、ウェブサービスに対して行われたリクエストの詳細なレコードを含めることができます。これらのログレコードは、セキュリティとアクセスの監査に役立つ場合があります。詳細については、「ログ (CloudWatch Logs)」を参照してください。

AWS CloudTrail アクションログ

App Runner は AWS CloudTrail、App Runner のユーザー、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、App Runner 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。CloudTrail コンソールで最新のイベントを表示し、証跡を作成して、Amazon Simple Storage Service (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。詳細については、「API アクション (CloudTrail)」を参照してください。

App Runner のコンプライアンス検証

サードパーティーの監査者は、複数の コンプライアンスプログラム AWS App Runner の一環として のセキュリティと AWS コンプライアンスを評価します。これらのプログラムには、SOC、PCI、FedRAMP、HIPAA などがあります。

AWS のサービス が特定のコンプライアンスプログラムの範囲内にあるかどうかを確認するには、「コンプライアンスAWS のサービス プログラムによる対象範囲内コンプライアンス」を参照し、関心のあるコンプライアンスプログラムを選択します。一般的な情報については、AWS「 Compliance ProgramsAssurance」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、「Downloading AWS Artifact Reports 」を参照してください。

を使用する際のお客様のコンプライアンス責任 AWS のサービス 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。 では、コンプライアンスに役立つ以下のリソース AWS を提供しています。

- セキュリティのコンプライアンスとガバナンス – これらのソリューション実装ガイドでは、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の機能をデプロイする手順を示します。
- HIPAA 対応サービスのリファレンス – HIPAA 対応サービスの一覧が提供されています。すべてが HIPAA 対応 AWS のサービス であるわけではありません。
- 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、お客様の業界と場所に適用される場合があります。
- AWS カスタマーコンプライアンスガイド – コンプライアンスの観点から責任共有モデルを理解します。このガイドは、複数のフレームワーク (米国国立標準技術研究所 (NIST)、Payment Card Industry Security Standards Council (PCI)、国際標準化機構 (ISO) を含む) のセキュリティコントロールを保護し、そのガイダンスに AWS のサービス マッピングするためのベストプラクティスをまとめたものです。
- 「 デベロッパーガイド」の「ルールによるリソースの評価」 – この AWS Config サービスは、リソース設定が社内プラクティス、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 Config
- AWS Security Hub – これにより AWS のサービス 、 内のセキュリティ状態を包括的に把握できます AWS。Security Hub では、セキュリティコントロールを使用して AWS リソースを評価し、セキュリティ業界標準とベストプラクティスに対するコンプライアンスをチェックします。サポートされているサービスとコントロールの一覧については、Security Hub のコントロールリファレンスを参照してください。
- Amazon GuardDuty – 環境をモニタリングして AWS アカウント不審なアクティビティや悪意のあるアクティビティがないか調べることで、、ワークロード、コンテナ、データに対する潜在的な脅威 AWS のサービス を検出します。GuardDuty を使用すると、特定のコンプライアンスフレームワークで義務付けられている侵入検知要件を満たすことで、PCI DSS などのさまざまなコンプライアンス要件に対応できます。
- AWS Audit Manager – これにより AWS のサービス 、 AWS 使用状況を継続的に監査し、リスクの管理方法と規制や業界標準への準拠を簡素化できます。

その他の App Runner セキュリティトピックについては、「」を参照してくださいセキュリティ。

App Runner 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 およびアベイラビリティーゾーンを中心に構築されています。 は、低レイテンシー、高スループット、および高度に冗長な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 AWS リージョンを提供します。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 および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。

AWS App Runner は、ユーザーに代わって AWS グローバルインフラストラクチャの使用を管理および自動化します。App Runner を使用すると、 AWS が提供する可用性と耐障害性メカニズムのメリットが得られます。

その他の App Runner セキュリティトピックについては、「」を参照してくださいセキュリティ。

のインフラストラクチャセキュリティ AWS App Runner

マネージドサービスである AWS App Runner 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」に記載されている AWS グローバルネットワークセキュリティの手順で保護されています。

AWS が公開した API コールを使用して、ネットワーク経由で App Runner にアクセスします。クライアントは、Transport Layer Security (TLS) 1.2 以降をサポートする必要があります。クライアントは、Ephemeral Diffie-Hellman (DHE) や Elliptic Curve Ephemeral Diffie-Hellman (ECDHE) などの Perfect Forward Secrecy (PFS) を使用する暗号スイートもサポートする必要があります。これらのモードは、Java 7 以降など、最近のほとんどのシステムでサポートされています。

また、リクエストにはアクセスキー ID と、IAM プリンシパルに関連付けられているシークレットアクセスキーを使用して署名する必要があります。またはAWS Security Token Service (AWS STS) を使用して、一時的なセキュリティ認証情報を生成し、リクエストに署名することもできます。

その他の App Runner セキュリティトピックについては、「」を参照してくださいセキュリティ。

VPC エンドポイントでの App Runner の使用

AWS アプリケーションは、Amazon Virtual Private Cloud (Amazon VPC) から VPC で AWS のサービス 実行される他の AWS App Runner サービスとサービスを統合する場合があります。アプリケーションの一部は、VPC 内から App Runner にリクエストを行う場合があります。たとえば、 AWS CodePipeline を使用して App Runner サービスに継続的にデプロイできます。アプリケーションのセキュリティを向上させる 1 つの方法は、これらの App Runner リクエスト (および他のリクエスト AWS のサービス) を VPC エンドポイント経由で送信することです。

VPC エンドポイントを使用すると、 を使用するサポートされている AWS のサービス および VPC エンドポイントサービスに VPC をプライベートに接続できます AWS PrivateLink。インターネットゲートウェイ、NAT デバイス、VPN 接続、または AWS Direct Connect 接続は必要ありません。

VPC 内のリソースは、パブリック IP アドレスを使用して App Runner リソースとやり取りしません。VPC と App Runner 間のトラフィックは Amazon ネットワークを離れません。VPC エンドポイントの詳細については、「 AWS PrivateLink ガイド」の「VPC エンドポイント」を参照してください。

> **Note**
>
> デフォルトでは、App Runner サービスのウェブアプリケーションは、App Runner が提供および設定する VPC で実行されます。この VPC はパブリックです。つまり、インターネットに接続されています。オプションで、アプリケーションをカスタム VPC に関連付けることができます。詳細については、「the section called “送信トラフィック”」を参照してください。
> サービスが VPC に接続されている場合でも、APIsを含む AWS インターネットにアクセスするようにサービスを設定できます。VPC アウトバウンドトラフィックのパブリックインターネットアクセスを有効にする方法については、「」を参照してくださいthe section called “サブネットを選択する際の考慮事項 ”。
> App Runner は、アプリケーションの VPC エンドポイントの作成をサポートしていません。

App Runner の VPC エンドポイントの設定

VPC で App Runner サービスのインターフェイス VPC エンドポイントを作成するには、「 AWS PrivateLink ガイド」の「インターフェイスエンドポイントの作成」の手順に従います。[Service Name] (サービス名)には `com.amazonaws.`*`region`*`.apprunner` を選択します。

VPC ネットワークプライバシーに関する考慮事項

> **Important**
>
> App Runner に VPC エンドポイントを使用しても、VPC からのすべてのトラフィックがインターネット外に留まるとは限りません。VPC はパブリックである可能性があります。さらに、ソリューションの一部では、VPC エンドポイントを使用して AWS API コールを実行しない場合があります。たとえば、パブリックエンドポイントを使用して他の サービスを呼び出す AWS のサービス ことができます。VPC のソリューションにトラフィックプライバシーが必要な場合は、このセクションをお読みください。

VPC 内のネットワークトラフィックのプライバシーを確保するには、次の点を考慮してください。

- DNS 名を有効にする – アプリケーションの一部は、`apprunner.`*`region`*`.amazonaws.com`パブリックエンドポイントを使用してインターネット経由で App Runner にリクエストを送信する場合があります。VPC がインターネットアクセスで設定されている場合、これらのリクエストはユーザーに通知されずに成功します。これを防ぐには、エンドポイントの作成時に DNS 名の有効化が有効になっていることを確認します。デフォルトでは、true に設定されています。これにより、パブリックサービスエンドポイントをインターフェイス VPC エンドポイントにマップする DNS エントリが VPC に追加されます。
- 追加サービス用に VPC エンドポイントを設定する – ソリューションは他の にリクエストを送信する場合があります AWS のサービス。例えば、 は にリクエストを送信する AWS CodePipeline 場合があります AWS CodeBuild。これらのサービスの VPC エンドポイントを設定し、これらのエンドポイントで DNS 名を有効にします。
- プライベート VPC を設定する – 可能な場合 (ソリューションがインターネットアクセスをまったく必要としない場合) 、VPC をプライベートとして設定します。これは、インターネット接続がないことを意味します。これにより、VPC エンドポイントが欠落していると エラーが表示されるため、欠落しているエンドポイントを追加できます。

エンドポイントポリシーを使用して VPC エンドポイントでアクセスを制御する

VPC エンドポイントポリシーは App Runner でサポートされています。デフォルトでは、インターフェイスエンドポイントを介して App Runner へのフルアクセスが許可されます。VPC エンドポイントポリシーを使用して、App Runner エンドポイントにアクセスできる AWS プリンシパルを制御

できます。または、セキュリティグループをエンドポイントネットワークインターフェイスに関連付けて、インターフェイスエンドポイントを介して App Runner へのトラフィックを制御することもできます。

インターフェイスエンドポイントとの統合

App Runner は、App Runner へのプライベート接続を提供し AWS PrivateLink、インターネットへのトラフィックの露出を排除する App Runner をサポートしています。を使用してアプリケーションが App Runner にリクエストを送信できるようにするには AWS PrivateLink、インターフェイスエンドポイントと呼ばれる VPC エンドポイントのタイプを設定します。詳細については、「AWS PrivateLink 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。

App Runner での設定と脆弱性の分析

AWS とお客様は、ソフトウェアコンポーネントのセキュリティとコンプライアンスの高レベルを達成する責任を共有します。詳細については、 AWS 「 責任共有モデル」を参照してください。

パッチコンテナイメージ

コンテナイメージへのパッチ適用は、共有セキュリティモデルにおけるお客様の責任の一部です。イメージ所有者は、コンテナイメージを更新し、定期的にパッチを適用する責任があります。コンテナイメージの更新を確認して適用するための定期的なスケジュールを設定することをお勧めします。イメージの脆弱性をスキャンする方法の詳細については、AWS App Runner ドキュメントを参照してください。

その他の App Runner セキュリティトピックについては、「」を参照してくださいセキュリティ。

App Runner のセキュリティのベストプラクティス

AWS App Runner には、独自のセキュリティポリシーを開発および実装する際に考慮すべきいくつかのセキュリティ機能が用意されています。以下のベストプラクティスは一般的なガイドラインであり、完全なセキュリティソリューションに相当するものではありません。これらのベストプラクティスはお客様の環境に適切ではないか、十分ではない場合があるため、絶対的な解決策ではなく、役に立つ情報としてお考えください。

その他の App Runner セキュリティトピックについては、「」を参照してくださいセキュリティ。

予防的セキュリティのベストプラクティス

予防的セキュリティ管理では、インシデントが発生する前に防ぐことを試みます。

最小特権アクセスの実装

App Runner は、IAM ユーザーとアクセスロールに AWS Identity and Access Management (IAM) 管理ポリシーを提供します。 ???これらの管理ポリシーは、App Runner サービスの正しいオペレーションに必要なすべてのアクセス許可を指定します。

アプリケーションで、管理ポリシーのすべてのアクセス権限が必要とは限りません。カスタマイズして、ユーザーと App Runner サービスがタスクを実行するために必要なアクセス許可のみを付与できます。これは特に、ユーザーロールごとに異なるアクセス権限のニーズを持つユーザーポリシーに関連します。最小特権アクセスの実装は、セキュリティリスクと、エラーや悪意によってもたらされる可能性のある影響の低減における基本です。

イメージをスキャンして脆弱性がないか調べる

Amazon ECR の APIs を使用して、コンテナイメージ内のソフトウェアの脆弱性を特定できます。詳細については、「Amazon S3 のドキュメント」参照してください。

セキュリティ問題の検出ベストプラクティス

セキュリティコントロールの検出により、セキュリティ違反が発生した後に識別されます。セキュリティ上の脅威やインシデントの検出に役立ちます。

モニタリングを実装する

モニタリングは、App Runner ソリューションの信頼性、セキュリティ、可用性、パフォーマンスを維持する上で重要な部分です。 は、 AWS サービスのモニタリングに役立ついくつかのツールとサービス AWS を提供します。

以下は、モニタリングする項目のいくつかの例です。

- App Runner の Amazon CloudWatch メトリクス – 主要な App Runner メトリクスとアプリケーションのカスタムメトリクスのアラームを設定します。詳細については、「メトリクス (CloudWatch)」を参照してください。
- AWS CloudTrail エントリ – `PauseService`や など、可用性に影響を与える可能性のあるアクションを追跡します`DeleteConnection`。詳細については、「API アクション (CloudTrail)」を参照してください。

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。